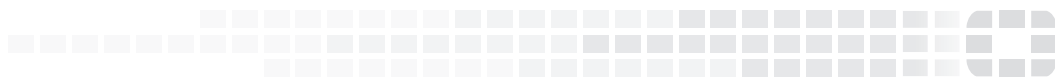




FORTINET
High Performance Network Security



FortiOS™ Handbook - VM Installation

Version 5.4



FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FORTINET PRIVACY POLICY

<https://www.fortinet.com/corporate/about-us/privacy.html>

FEEDBACK

Email: techdocs@fortinet.com



Tuesday, January 9, 2018

FortiOS™ Handbook - VM Installation

01-540-203906-20140130

TABLE OF CONTENTS

Change Log	5
Introduction	6
Document scope	6
What's new in VM in 5.4	7
New Features in 5.4.1	7
FortiGate VM cloud-init integration (300398)	7
Allow VM tools (VMWare platform) to set network settings for FortiGate VMS (292248)	7
FortiKVM removed from most FortiGates (366859)	8
FortiKVM support added to select models (282335)	8
FGT-VM VMX (v2) (306438)	8
FortiOS On-Demand (308130)	8
New Features in 5.4.0	9
Changes to FG-VM00 Min/Max Values (246780,372030)	9
Integrate VMtools Into FortiGate-VM for VMware (248842)	9
VM License Check Time Extension (262494)	9
FortiGate VM Single Root I/O Virtualization (SR-IOV) support (275432)	9
You can reset FortiGate VMs to factory defaults without deleting the VM license (280471)	9
FortiGate VM Overview	10
FortiGate VM models and licensing	10
FortiGate VM evaluation license	11
Registering FortiGate VM with Customer Service & Support	11
Downloading the FortiGate VM deployment package	11
Deployment package contents	13
Citrix XenServer	13
OpenXEN	13
Microsoft Hyper-V	13
KVM	13
VMware ESX/ESXi	13
Deploying the FortiGate VM appliance	14
Deployment example – VMware	15
Open the FortiGate VM OVF file with the vSphere client	15
Configure FortiGate VM hardware settings	20
Transparent mode VMware configuration	22

High Availability VMware configuration	23
Power on your FortiGate VM	23
Deployment example – MS Hyper-V	24
Create the FortiGate VM virtual machine	24
Configure FortiGate VM hardware settings	31
FortiGate VM virtual processors	33
FortiGate VM network adapters	34
FortiGate VM virtual hard disk	35
High Availability Hyper-V configuration	43
Start the FortiGate VM	43
Deployment example – KVM	44
Create the FortiGate VM virtual machine	44
Configure FortiGate VM hardware settings	46
Start the FortiGate VM	47
Deployment example – OpenXen	48
Create the FortiGate VM virtual machine (VMM)	48
Deployment example – Citrix XenServer	54
Create the FortiGate VM virtual machine (XenCenter)	54
Configure virtual hardware	58
Configuring number of CPUs and memory size	58
Configuring disk storage	59
FortiGate VM Initial Configuration	61
Set FortiGate VM port1 IP address	61
Connect to the FortiGate VM Web-based Manager	64
Upload the FortiGate VM license file	64
CLI	65
Validate the FortiGate VM license with FortiManager	65
To validate your FortiGate VM with your FortiManager:	65

Change Log

Date	Change Description
2018-01-09	Added CLI info on license installation. Changed screen shot for VM license upload. Addition information added about license status.
2017-10-31	Information added on geographic addresses.
2017-10-26	Correction regarding New Feature Listing. Added information on Licensing timeout.
2017-05-26	Reference to HSTS in SSL inspection
2017-05-09	Correction regarding activating the FMG license. Caution on virtual NIC limitations.
2016-10-31	Initial Release.

Introduction

FortiGate virtual appliances allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. FortiGate virtual appliances feature all of the security and networking services common to traditional hardware-based FortiGate appliances. With the addition of virtual appliances from Fortinet, you can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform.

Document scope

This document describes how to deploy a FortiGate virtual appliance in several virtualization server environments. This includes how to configure the virtual hardware settings of the virtual appliance.

This document assumes:

- you have already successfully installed the virtualization server on the physical machine,
- you have installed appropriate VM management software on either the physical server or a computer to be used for VM management.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For these issues, see the FortiGate 5.2 Handbook.

This document includes the following sections:

- [FortiGate VM Overview](#)
- [Deployment example – VMware](#)
- [Deployment example – MS Hyper-V](#)
- [Deployment example – KVM](#)
- [Deployment example – OpenXen](#)
- [Deployment example – Citrix XenServer](#)

What's new in VM in 5.4

New Features in 5.4.1

FortiGate VM cloud-init integration (300398)

Cloud-init is a set of python scripts and utilities commonly used for multi-distribution of VMs into cloud environments.

With cloud-init integration, when users launch a new instance of Fortigate VM, they can:

- Upload a license to a FGT-VM
- Provide initial management configuration, e.g. IP, default gateway, DNS
- Set port configuration mode (DHCP or static)
- Provision initial firewall policies

Cloud-init documentation can be found at <https://cloudinit.readthedocs.io/en/latest/>

Allow VM tools (VMWare platform) to set network settings for FortiGate VMS (292248)

Changes have been made to the firmware to mitigate the following issues:

- FGVM does not allow IP configuration during deployment.
- The use of multiple OVF files for different network adapter types is redundant.
- The sequence of interfaces is not kept in consistent with network adapters in VM settings.

These issues are corrected by the following changes:

- During deployment, the user will be prompted for an IP allocation policy (when using the new vApp OVF file). Static/DHCP can be selected for each port. Gateway can be configured for port1. Hostname, as well as primary/secondary DNS address, can be configured.
- During deployment, the user will be able to select either E1000 virtual network adapter or VMXNET3 ones (when using the new vApp OVF file).
- The new process keeps FGTVM's interface in the same sequence as the order shown in VM settings.
- There is an added CLI command `"diag vmware show-ovfenv"` to print out the whole OVF environment.

All additional features during deployment are only available when FGTVM is deployed through vCenter as a vApp.

- FGTVM interface sequence is determined with the following logic (and priority):
 - If OVF environment is available, the sequence present in the OVF environment will be used. (This is the preferred case. As the sequence can kept consistent with VM settings, regardless of whether adapters are removed/added, or mixed types of adapters are used.)
 - If the first network adapter is VMXNET3, FGTVM will use a dynamic mapping of interface, according to the total number of network adapters present. (This assumes all the network adapters are VMXNET3.)
 - If the above conditions do not qualify, FGTVM will use a static mapping of interface, which assumes every network adapter is E1000

- Even when a fixed IP allocation policy is selected during deployment, DHCP might be enabled on port1. This happens when the interface IP is set to 0.0.0.0 on port1. Unfortunately, OVF environment is unable to provide which IP allocation policy has been selected. Rather, it is only able to give a set of IP/netmask on each of the interfaces.
- Configuration is applied AFTER IP allocation policy. This means, IP allocation policy works as default settings of interface, and is ignored when any existing configuration presents on a certain interface.

FortiKVM removed from most FortiGates (366859)

The FortiKVM feature that allowed a virtual instance of FortiGate on a FortiGate device is no longer part of FortiOS for most models. With few exceptions, this feature is being moved to FortiHypervisor, a specialised appliance with resources optimized for the purpose.

FortiKVM support added to select models (282335)

FortiKVM functionality is now available on the following models:

- FGT1500D
- FGT3700D
- FGT3700DX
- FGT3810D

Interface assignment CLI:

```
config system vm
  edit 0
    set name vm1
    config interface
      edit 1
        set name vnic1
        set device [physical | vlan | softswitch]
        mode [bridge | passthrough]
      end
    end
  end
end
```

[device]: can assign physical, VLAN, or softwitch type host interface to this attribute.

[mode]: this attribute is available only when device is assigned physical type interface, bridge mode means several vNIC can share this interface, when packet arrives, host will lookup vNIC by dst mac address, in passthrough mode, host will send all packets to the vNIC, only one vNIC can use the physical interface in passthrough mode.

FGT-VM VMX (v2) (306438)

FortiGate-VM VMX version 2 allows for automated deployment of virtual FortiGate instances running FortiOS 5.4.1 in a specific VMWare SDN environment. For more details read the Release Notes and Admin Guides for FortiGate-VM VMX.

FortiOS On-Demand (308130)

New VM platform to support a consumption based FOS VM pricing model. FortiOS On-Demand supports VMWare hypervisor, and Openstack KVM hypervisor platforms.

- These platforms have three interfaces only: mgmt, port1, and port2.
- port1 and port2 are used for metering, and is reported to a FortiManager via the updated process.
- The FortiManager is configured externally via Vapp for VMware or user-data in KVM.
- FortiGuard updates and webfiltering servers will initially point to the FortiManager.
- The FortiManager will authorize the FOSVM instance. If not authorized the vdom is disabled.

New Features in 5.4.0

Changes to FG-VM00 Min/Max Values (246780,372030)

- The maximum memory virtual memory has changed from 1 to 1.5 GB.
- The maximum number of VDOMs has changed from 1 to 2.

Integrate VMtools Into FortiGate-VM for VMware (248842)

The following VMtools sub set of features has been integrated into the FortiGate-VM for VMWare images:

- Start
- Stop
- Reboot
- IP state in vCenter

VM License Check Time Extension (262494)

VM license check time has been extended to 30 days, with daily warning notifications and a counter.

FortiGate VM Single Root I/O Virtualization (SR-IOV) support (275432)

SR-IOV is a specification that allows a PCIe device to be treated as multiple separate PCIe devices. This feature will enable better performance with Intel based servers across multiple VM platforms, including Citrix and AWS. In fact, AWS has optimized some instance types to take advantage of this feature.

You can reset FortiGate VMs to factory defaults without deleting the VM license (280471)

New command , **execute factoryreset keepvmlicense**, resets FortiGate VMs to factory defaults without deleting the VM license.

FortiGate VM Overview

The following topics are included in this section:

- [FortiGate VM models and licensing](#)
- [Registering FortiGate VM with Customer Service & Support](#)
- [Downloading the FortiGate VM deployment package](#)
- [Deployment package contents](#)
- [Deploying the FortiGate VM appliance](#)

FortiGate VM models and licensing

Fortinet offers the FortiGate VM in five virtual appliance models determined by license. When configuring your FortiGate VM, be sure to configure hardware settings within the ranges outlined below. Contact your Fortinet Authorized Reseller for more information.

FortiGate VM model information

Technical Specification	FG-VM00	FG-VM01	FG-VM02	FG-VM04	FG-VM08
Virtual CPUs (min / max)	1 / 1	1 / 1	1 / 2	1 / 4	1 / 8
Virtual Network Interfaces (min / max)			2 / 10		
Virtual Memory (min / max)	1GB / 1.5GB	1GB / 2GB	1GB / 4GB	1GB / 6GB	1GB /12GB
Virtual Storage (min / max)			32GB / 2TB		
Managed Wireless APs (tunnel mode / global)	32 / 32	32 / 64	256 / 512	256 / 512	1024 / 4096
Virtual Domains (default / max)	1 / 2	10 / 10	10 / 25	10 / 50	10 / 250



There may be times the min/max values can change. An example for this is when the maximum memory for FG-VM00 changed between 5.2 and 5.4 from 1 GB to 1.5 GB. If that is the case, the settings for the VM will have to be manually changed to accommodate the new parameters.

After placing an order for FortiGate VM, a license registration code is sent to the email address used on the order form. Use the registration number provided to register the FortiGate VM with Customer Service & Support and

then download the license file. Once the license file is uploaded to the FortiGate VM and validated, your FortiGate VM appliance is fully functional.



The number of Virtual Network Interfaces is not solely dependent on the FortiGate VM. Some virtual environments have their own limitations on the number of interfaces allowed. As an example, if you go to <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-multiple-nics>, you will find that Azure has its own restrictions for VMs, depending on the type of deployment or even the size of the VM.

FortiGate VM evaluation license

FortiGate VM includes a limited embedded 15-day trial license that supports:

- 1 CPU maximum
- 1024 MB memory maximum
- low encryption only (no HTTPS administrative access)
- all features except FortiGuard updates

You cannot upgrade the firmware, doing so will lock the Web-based Manager until a license is uploaded. Technical support is not included. The trial period begins the first time you start FortiGate VM. After the trial license expires, functionality is disabled until you upload a license file.

Registering FortiGate VM with Customer Service & Support

To obtain the FortiGate VM license file you must first register your FortiGate VM with [Customer Service & Support](#).

To register your FortiGate VM:

1. Log in to the Customer Service & Support portal using an existing support account or select **Sign Up** to create a new account.
2. In the main page, under **Asset**, select **Register/Renew**.

The **Registration** page opens.

3. Enter the registration code that was emailed to you and select **Register**. A registration form will display.
4. After completing the form, a registration acknowledgement page will appear.
5. Select the **License File Download** link.
6. You will be prompted to save the license file (.lic) to your local computer. See "Upload the license file" for instructions on uploading the license file to your FortiGate VM via the Web-based Manager.

Downloading the FortiGate VM deployment package

FortiGate VM deployment packages are included with FortiGate firmware images on the [Customer Service & Support](#) site. First, see the following table to determine the appropriate VM deployment package for your VM platform.

Selecting the correct FortiGate VM deployment package for your VM platform

VM Platform	FortiGate VM Deployment File
Citrix XenServer v5.6sp2, 6.0 and later	FGT_VM64-v500-buildnnnn-FORTINET.out.CitrixXen.zip
OpenXen v3.4.3, 4.1	FGT_VM64-v500-buildnnnn-FORTINET.out.OpenXen.zip
Microsoft Hyper-V Server 2008R2 and 2012	FGT_VM64-v500-buildnnnn-FORTINET.out.hyperv.zip
KVM (qemu 0.12.1)	FGT_VM64-v500-buildnnnn-FORTINET.out.kvm.zip
VMware ESX 4.0, 4.1 ESXi 4.0/4.1/5.0/5.1/5.5	FGT_VM32-v500-buildnnnn-FORTINET.out.ovf.zip (32-bit) FGT_VM64-v500-buildnnnn-FORTINET.out.ovf.zip

For more information see the FortiGate product datasheet available on the Fortinet web site, <http://www.fortinet.com/products/fortigate/virtualappliances.html>.

The firmware images FTP directory is organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FGT_VM32-v500-build0151-FORTINET.out.ovf.zip image found in the v5.0 Patch Release 2 directory is specific to the FortiGate VM 32-bit environment.



You can also download the FortiOS Release Notes, FORTINET-FORTIGATE MIB file, FSSO images, and SSL VPN client in this directory. The Fortinet Core MIB file is located in the main FortiGate v5.00 directory.

To download the FortiGate VM deployment package:

1. In the main page of the Customer Service & Support site, select **Download > Firmware Images**.

The **Firmware Images** page opens.

2. In the **Firmware Images** page, select **FortiGate**.
3. Browse to the appropriate directory on the FTP site for the version that you would like to download.
4. Download the appropriate .zip file for your VM server platform.

You can also download the FortiGate Release Notes.

5. Extract the contents of the deployment package to a new file folder.

Deployment package contents

Citrix XenServer

The FORTINET.out.CitrixXen.zip file contains:

- fortios.vhd: the FortiGate VM system hard disk in VHD format
- fortios.xva: binary file containing virtual hardware configuration settings
- in the ovf folder:
 - FortiGate-VM64.ovf: Open Virtualization Format (OVF) template file, containing virtual hardware settings for Xen
 - fortios.vmdk: the FortiGate VM system hard disk in VMDK format
 - datadrive.vmdk: the FortiGate VM log disk in VMDK format

The ovf folder and its contents is an alternative method of installation to the .xva and VHD disk image.

OpenXEN

The FORTINET.out.OpenXen.zip file contains only fortios.qcow2, the FortiGate VM system hard disk in qcow2 format. You will need to manually:

- create a 32GB log disk
- specify the virtual hardware settings

Microsoft Hyper-V

The FORTINET.out.hyperv.zip file contains:

- in the Virtual Hard Disks folder:
 - fortios.vhd: the FortiGate VM system hard disk in VHD format
 - DATADRIVE.vhd: the FortiGate VM log disk in VHD format
- In the Virtual Machines folder:
 - fortios.xml: XML file containing virtual hardware configuration settings for Hyper-V. This is compatible with Windows Server 2012.
- Snapshots folder: optionally, Hyper-V stores snapshots of the FortiGate VM state here

KVM

The FORTINET.out.kvm.zip contains only fortios.qcow2, the FortiGate VM system hard disk in qcow2 format. You will need to manually:

- create a 32GB log disk
- specify the virtual hardware settings

VMware ESX/ESXi

You will need to create a 32GB log disk.

The FORTINET.out.ovf.zip file contains:

- fortios.vmdk: the FortiGate VM system hard disk in VMDK format
- datadrive.vmdk: the FortiGate VM log disk in VMDK format
- Open Virtualization Format (OVF) template files:
 - FortiGate-VM64.ovf: OVF template based on Intel e1000 NIC driver
 - FortiGate-VM64.hw04.ovf: OVF template file for older (v3.5) VMware ESX server
 - FortiGate-VMxx.hw07_vmxnet2.ovf: OVF template file for VMware vmxnet2 driver
 - FortiGate-VMxx.hw07_vmxnet3.ovf: OVF template file for VMware vmxnet3 driver



Use the VMXNET3 interface (FortiGate-VMxx.hw07_vmxnet3.ovf template) if the virtual appliance will distribute workload to multiple processor cores.

Deploying the FortiGate VM appliance

Prior to deploying the FortiGate VM appliance, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiGate VM assume that

- You are familiar with the management software and terminology of your VM platform.
- An Internet connection is available for FortiGate VM to contact FortiGuard to validate its license or, for closed environments, a FortiManager can be contacted to validate the FortiGate VM license. See "Validate the FortiGate VM license with FortiManager".

For assistance in deploying FortiGate VM, refer to the deployment chapter in this guide that corresponds to your VMware environment. You might also need to refer to the documentation provided with your VM server. The deployment chapters are presented as examples because for any particular VM server there are multiple ways to create a virtual machine. There are command line tools, APIs, and even alternative graphical user interface tools.

Before you start your FortiGate VM appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiGate VM, you will have access only through the console window of your VM server environment. After you configure one FortiGate network interface with an IP address and administrative access, you can access the FortiGate VM web-based manager.

After deployment and license validation, you can upgrade your FortiGate VM appliance's firmware by downloading either FGT_VM32-v500-buildnnnn-FORTINET.out (32-bit) or FGT_VM64-v500-buildnnnn-FORTINET.out (64-bit) firmware. Firmware upgrading on a VM is very similar to upgrading firmware on a hardware FortiGate unit.

Deployment example – VMware

Once you have downloaded the FGT_VMxx-v5-build0xxx-FORTINET.out.ovf.zip file from <http://support.fortinet.com> and extracted the package contents to a folder on your local computer, you can use the vSphere client to create the virtual machine from the deployment package OVF template.

The following topics are included in this section:

[Open the FortiGate VM OVF file with the vSphere client](#)

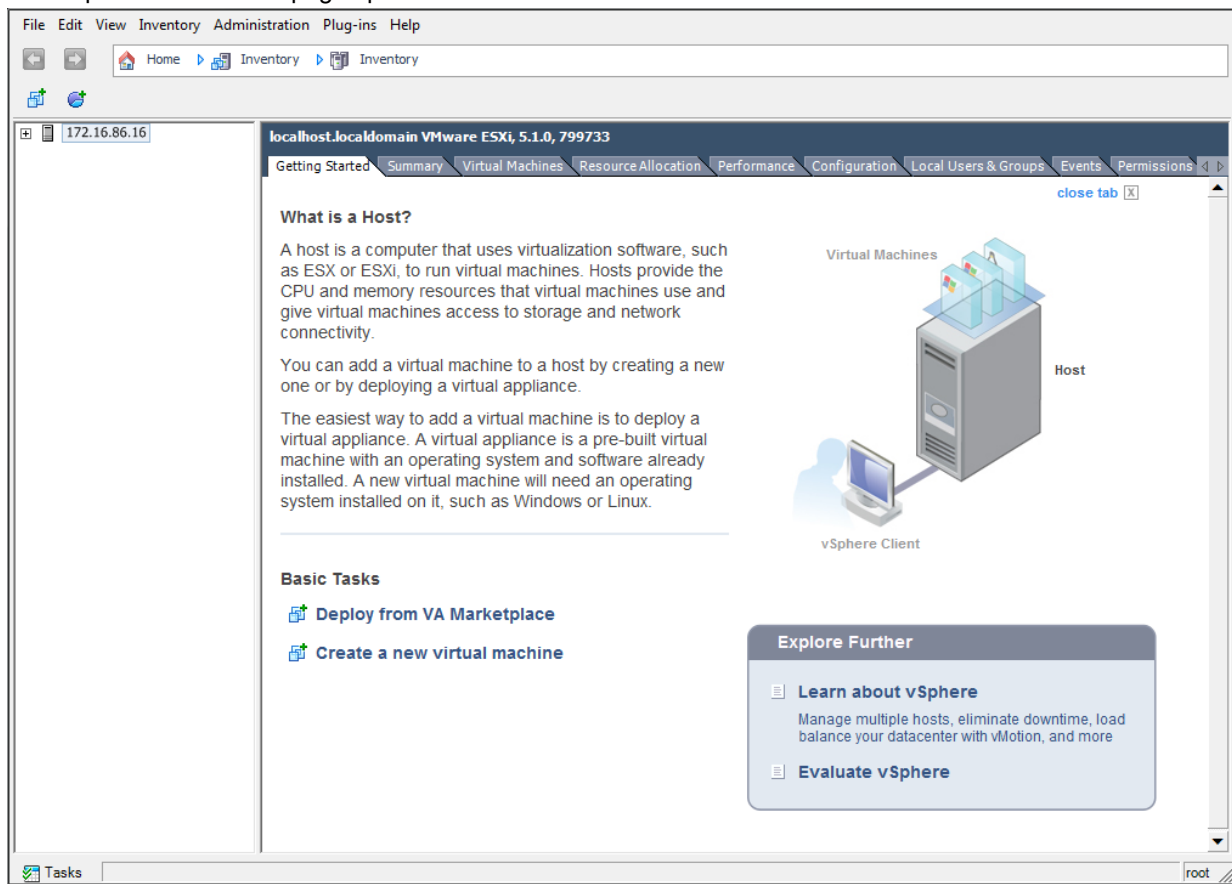
[Configure FortiGate VM hardware settings](#)

Open the FortiGate VM OVF file with the vSphere client

To deploy the FortiGate VM OVF template:

1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password and select **Login**.

The vSphere client home page opens.



2. Select **File > Deploy OVF Template** to launch the OVF Template wizard.

The OVF Template **Source** page opens.

3. Select the source location of the OVF file. Select **Browse** and locate the OVF file on your computer. Select **Next** to continue.

The OVF Template **Details** page opens.

OVF Template Details
Verify OVF template details.

[Source](#)
OVF Template Details
End User License Agreement
Name and Location
Disk Format
Network Mapping
Ready to Complete

Product:	Fortigate-VM
Version:	
Vendor:	
Publisher:	No certificate present
Download size:	30.4 MB
Size on disk:	Unknown (thin provisioned) 32.0 GB (thick provisioned)
Description:	FortiGate Virtual Appliance by Fortinet Technologies Inc. (http://www.fortinet.com)

Help < Back Next > Cancel

4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Select **Next** to continue.

The OVF Template **End User License Agreement** page opens.

End User License Agreement
Accept the end user license agreements.

[Source](#)
[OVF Template Details](#)
End User License Agreement
Name and Location
Disk Format
Network Mapping
Ready to Complete

End User License Agreement for FortiGate Virtual Appliance

NOTICE TO ALL USERS: PLEASE READ THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CAREFULLY. FORTINET, INC. IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS LICENSE AGREEMENT AND DO NOT INSTALL THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE ON TANGIBLE MEDIA (e.g., CD) WITHOUT THE OPPORTUNITY TO REVIEW THIS LICENSE AND YOU DO NOT ACCEPT THIS LICENSE AGREEMENT, YOU MAY OBTAIN A REFUND OF THE AMOUNT YOU ORIGINALLY PAID IF YOU: (A) DO NOT USE THE SOFTWARE AND (B) RETURN IT, WITH PROOF OF PAYMENT, WITHIN THIRTY (30) DAYS OF THE PURCHASE DATE TO THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA) is an agreement between you and Fortinet, Inc. ("Fortinet"), which governs your use of this software product. A software license and a license key or "unlock code" ("Software License"), issued to a designated user only by Fortinet or its authorized agents, is required for each computer on which the Software is loaded.

Definitions: (a) "Software" means (a) all means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) with which this Agreement is provided or such contents as are hosted by Fortinet or its distributors, resellers, OEM/MSP partners, or other business partners (collectively "Authorized Partner(s)"), including but not limited to (i) Fortinet or third party computer information or software; (ii) related explanatory materials in printed, electronic, or online form ("Documentation"); and (b) upgrades, modified or subsequent versions and updates (collectively "Updates"), and Software, if any, licensed to you by Fortinet or an

Accept

Help

< Back Next > Cancel

5. Read the end user license agreement for FortiGate VM. Select **Accept** and then select **Next** to continue.

The OVF Template **Name and Location** page opens.

Name and Location
Specify a name and location for the deployed template

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
Name and Location
[Disk Format](#)
[Network Mapping](#)
[Ready to Complete](#)

Name:
Fortigate-VM-01
The name can contain up to 80 characters and it must be unique within the inventory folder.

Help < Back Next > Cancel

6. Enter a name for this OVF template. The name can contain up to 80 characters and it must be unique within the inventory folder. Select **Next** to continue.

The OVF Template **Disk Format** page opens.

Disk Format
In which format do you want to store the virtual disks?

Source
OVF Template Details
End User License Agreement
Name and Location
Disk Format
Network Mapping
Ready to Complete

Datastore: datastore 1

Available space (GB): 394.6

☒ Thick Provision Lazy Zeroed
☐ Thick Provision Eager Zeroed
☐ Thin Provision

Help < Back Next > Cancel

7. Select one of the following:
 - **Thick Provision Lazy Zeroed:** Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
 - **Thick Provision Eager Zeroed:** Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
 - **Thin Provision:** Allocates the disk space only when a write occurs to a block, but the total volume size is reported by VMFS to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains on the volume regardless if you have deleted data, etc.
8. Select **Next** to continue.

The OVF Template **Network Mapping** page opens.

Network Mapping
What networks should the deployed template use?

[Source](#)
[OVF Template Details](#)
[End User License Agreement](#)
[Name and Location](#)
[Disk Format](#)
Network Mapping
Ready to Complete

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Network 1	VM Network
Network 2	VM Network
Network 3	VM Network
Network 4	VM Network
Network 5	VM Network
Network 6	VM Network
Network 7	VM Network

Description:
The VM Network network

Warning: Multiple source networks are mapped to the host network: VM Network

[Help](#) [< Back](#) [Next >](#) [Cancel](#)

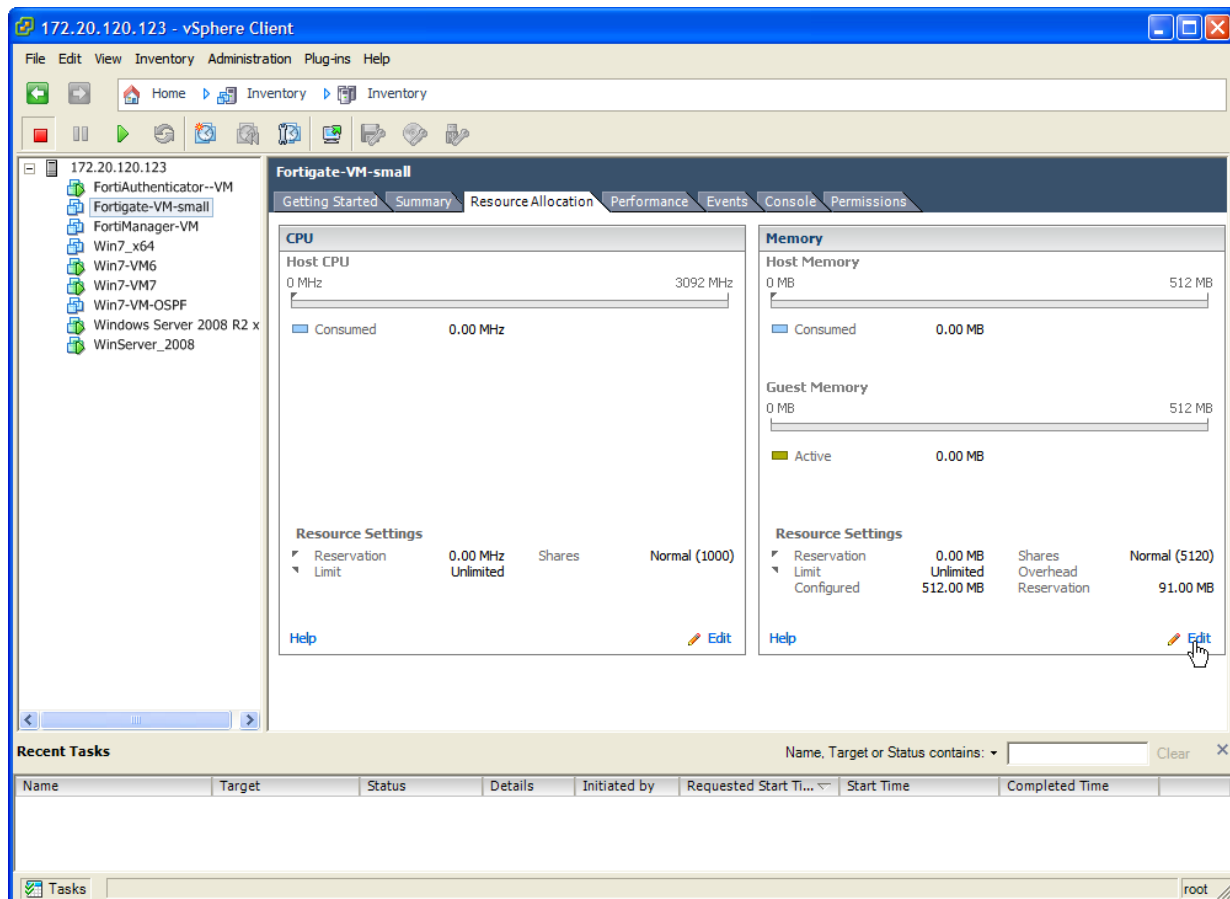
- Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiGate VM. You must set the destination network for this entry to access the device console. Select **Next** to continue.

The OVF Template **Ready to Complete** page opens.

- Review the template configuration. Make sure that **Power on after deployment** is not enabled. You might need to configure the FortiGate VM hardware settings prior to powering on the FortiGate VM.
- Select **Finish** to deploy the OVF template. You will receive a **Deployment Completed Successfully** dialog box once the FortiGate VM OVF template wizard has finished.

Configure FortiGate VM hardware settings

Before powering on your FortiGate VM you must configure the virtual memory, virtual CPU, and virtual disk configuration to match your FortiGate VM license.



Transparent mode VMware configuration

If you want to use your FortiGate-VM in transparent mode, your VMware server's virtual switches must operate in promiscuous mode. This permits these interfaces to receive traffic that will pass through the FortiGate unit but was not addressed to the FortiGate unit.

In VMware, promiscuous mode must be explicitly enabled:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of vSwitch0.
4. In the **Properties** window left pane, select **vSwitch** and then select **Edit**.
5. Select the **Security** tab, set **Promiscuous Mode** to **Accept**, then select **OK**.
6. Select **Close**.
7. Repeat steps 3 through 6 for other vSwitches that your transparent mode FortiGate-VM uses.

High Availability VMware configuration

If you want to combine two or more FortiGate-VM instances into a FortiGate Clustering Protocol (FGCP) High Availability (HA) cluster the VMware server's virtual switches used to connect the heartbeat interfaces must operate in promiscuous mode. This permits HA heartbeat communication between the heartbeat interfaces. HA heartbeat packets are non-TCP packets that use Ethertype values 0x8890, 0x8891, and 0x8890. The FGCP uses link-local IPv4 addresses in the 169.254.0.x range for HA heartbeat interface IP addresses.

To enable promiscuous mode in VMware:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of a virtual switch used to connect heartbeat interfaces.
4. In the **Properties** window left pane, select **vSwitch** and then select **Edit**.
5. Select the **Security** tab, set **Promiscuous Mode** to **Accept**, then select **OK**.
6. Select **Close**.

You must also set the virtual switches connected to other FortiGate interfaces to allow MAC address changes and to accept forged transmits. This is required because the FGCP sets virtual MAC addresses for all FortiGate interfaces and the same interfaces on the different VM instances in the cluster will have the same virtual MAC addresses.

To make the required changes in VMware:

1. In the vSphere client, select your VMware server in the left pane and then select the **Configuration** tab in the right pane.
2. In **Hardware**, select **Networking**.
3. Select **Properties** of a virtual switch used to connect FortiGate VM interfaces.
4. Set **MAC Address Changes** to **Accept**.
5. Set **Forged Transmits** to **Accept**.

Power on your FortiGate VM

You can now proceed to power on your FortiGate VM. There are several ways to do this:

- Select the name of the FortiGate VM you deployed in the inventory list and select **Power on the virtual machine** in the **Getting Started** tab.
- In the inventory list, right-click the name of the FortiGate VM you deployed, and select **Power > Power On**.
- Select the name of the FortiGate VM you deployed in the inventory list. Click the **Power On** button on the toolbar.

Select the Console tab to view the console. To enter text, you must click in the console pane. The mouse is then captured and cannot leave the console screen. As the FortiGate console is text-only, no mouse pointer is visible. To release the mouse, press Ctrl-Alt.

Deployment example – MS Hyper-V

Once you have downloaded the FGT_VMxx_HV-v5-build0xxx-FORTINET.out.hyperv.zip file and extracted the package contents to a folder on your Microsoft server, you can deploy the VHD package to your Microsoft Hyper-V environment.

The following topics are included in this section:

[Create the FortiGate VM virtual machine](#)

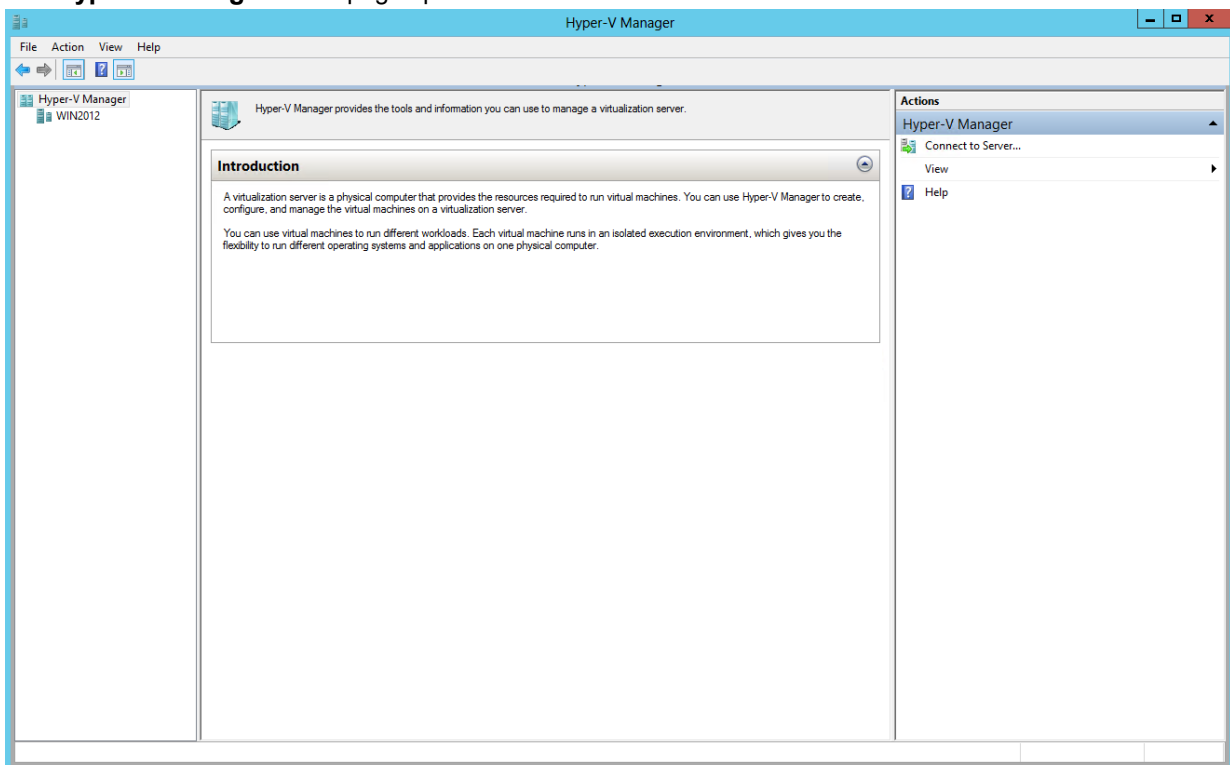
[Configure FortiGate VM hardware settings](#)

Create the FortiGate VM virtual machine

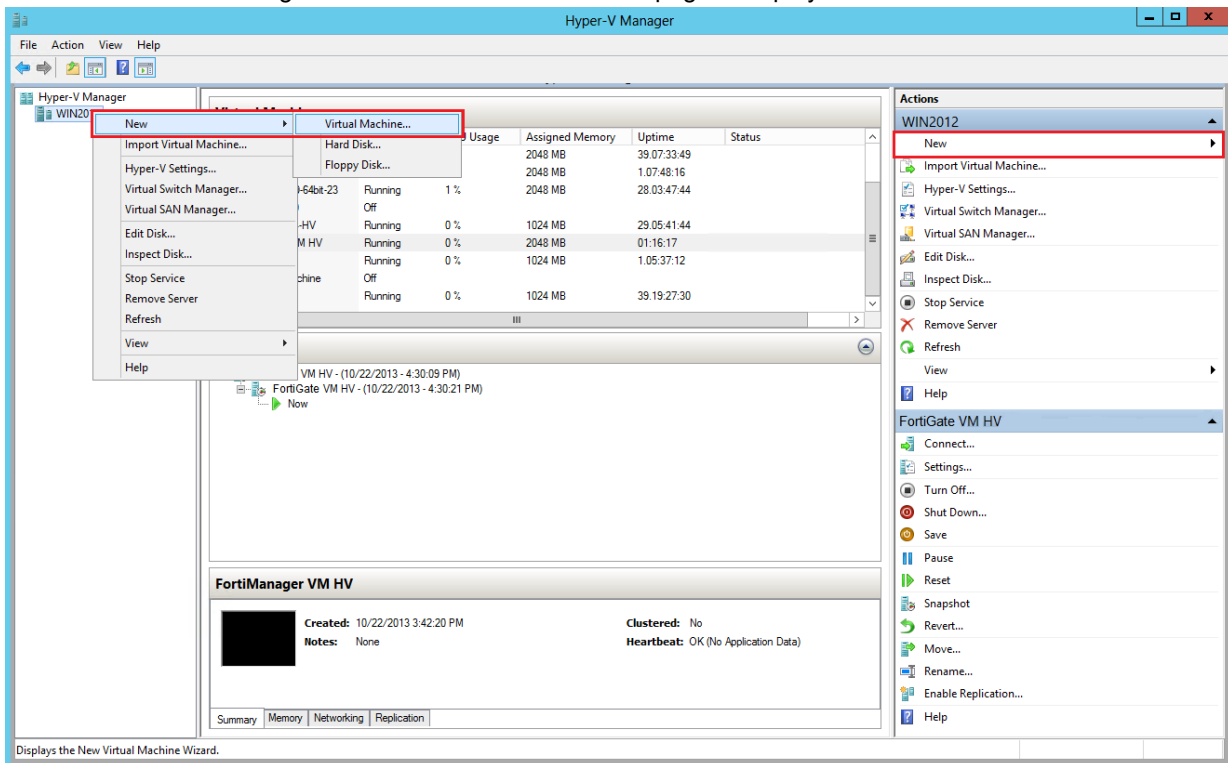
To create the FortiGate VM virtual machine:

1. Launch the Hyper-V Manager in your Microsoft server.

The **Hyper-V Manager** home page opens.

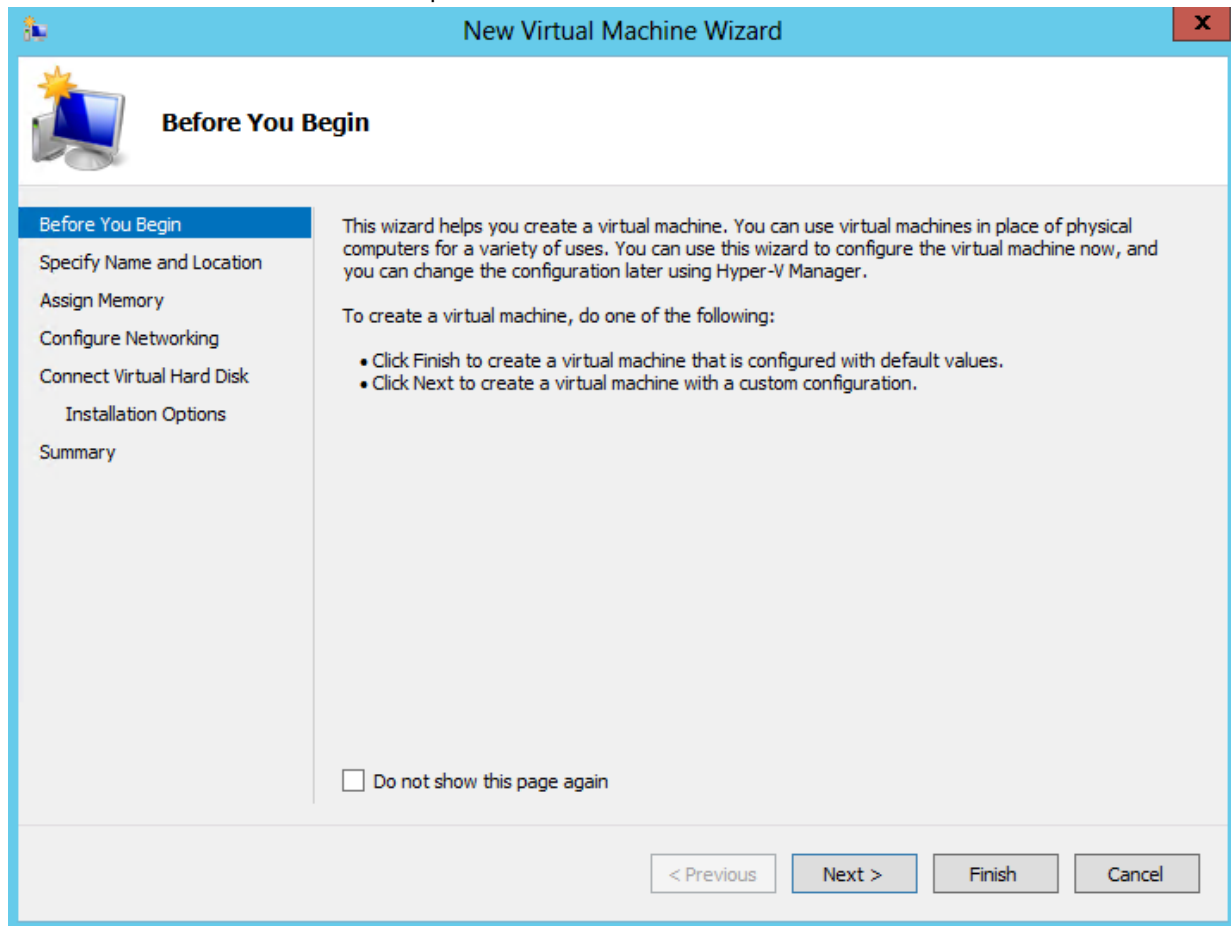


2. Select the server in the right-tree menu. The server details page is displayed.



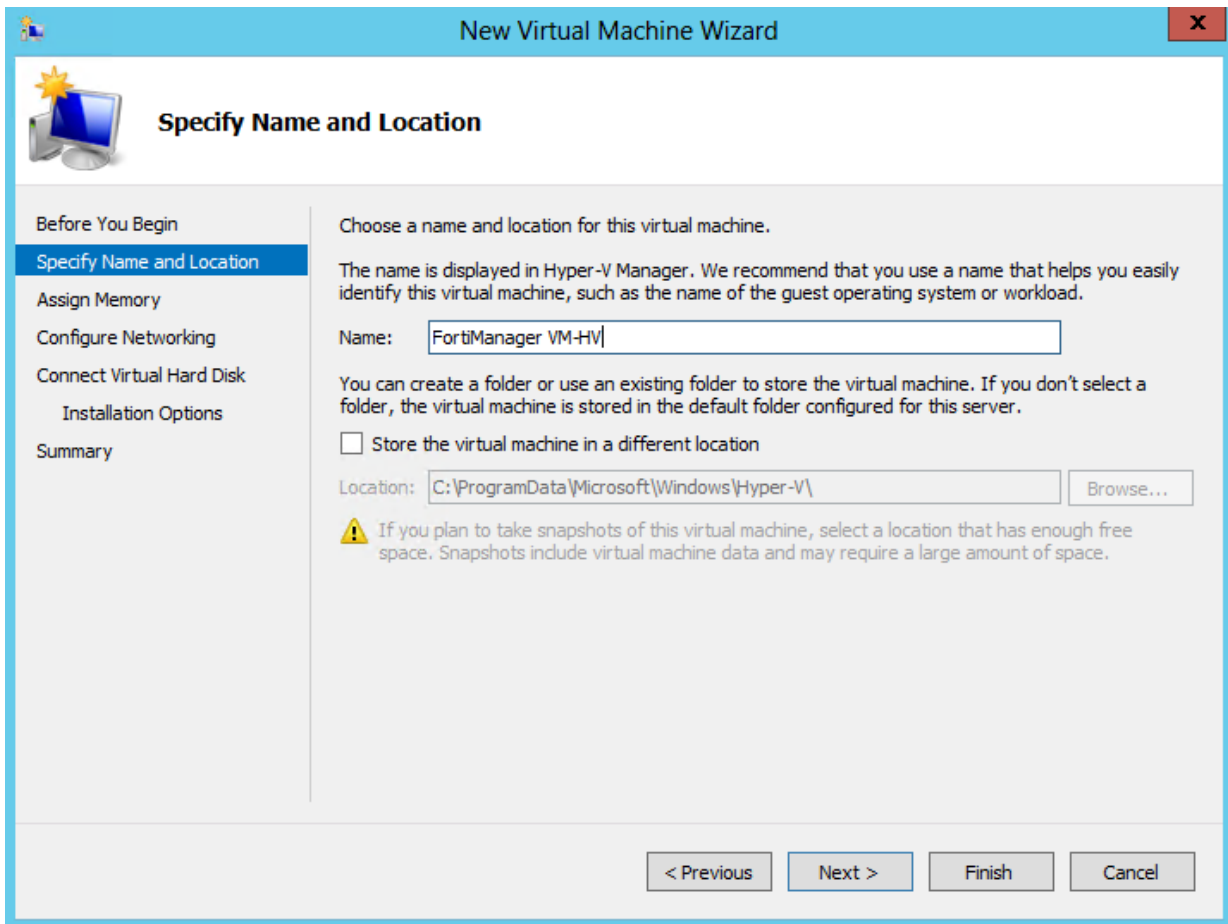
3. Right-click the server and select **New** and select **Virtual Machine** from the menu. Optionally, in the **Actions** menu, select **New** and select **Virtual Machine** from the menu.

The **New Virtual Machine Wizard** opens.



4. Select **Next** to create a virtual machine with a custom configuration.

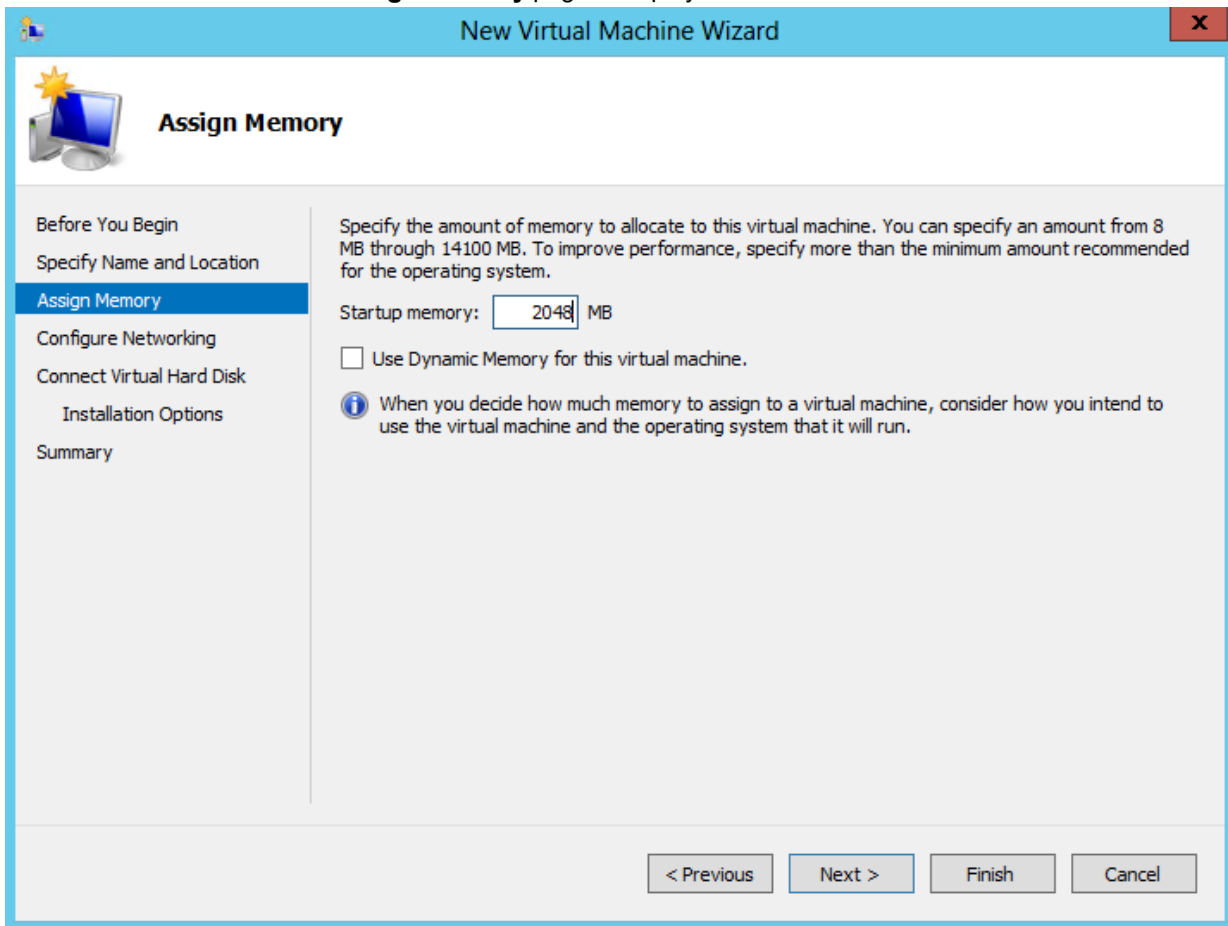
The **Specify Name and Location** page is displayed.



The screenshot shows the 'New Virtual Machine Wizard' window with the title bar 'New Virtual Machine Wizard' and a close button. The main window has a blue header bar with the title 'Specify Name and Location' and a small icon of a computer with a star. On the left, there is a navigation pane with the following steps: 'Before You Begin', 'Specify Name and Location' (highlighted), 'Assign Memory', 'Configure Networking', 'Connect Virtual Hard Disk', 'Installation Options', and 'Summary'. The main area contains the following text: 'Choose a name and location for this virtual machine.' followed by 'The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.' Below this is a text box labeled 'Name:' containing the text 'FortiManager VM-HV'. The next line says 'You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.' Below this is a checkbox labeled 'Store the virtual machine in a different location' which is unchecked. To the right of the checkbox is a text box labeled 'Location:' containing the text 'C:\ProgramData\Microsoft\Windows\Hyper-V\' and a 'Browse...' button. At the bottom of the main area is a warning icon and text: 'If you plan to take snapshots of this virtual machine, select a location that has enough free space. Snapshots include virtual machine data and may require a large amount of space.' At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

5. Enter a name for this virtual machine. The name is displayed in the Hyper-V Manager.

Select **Next** to continue. The **Assign Memory** page is displayed.



New Virtual Machine Wizard


Assign Memory

Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 8 MB through 14100 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: MB

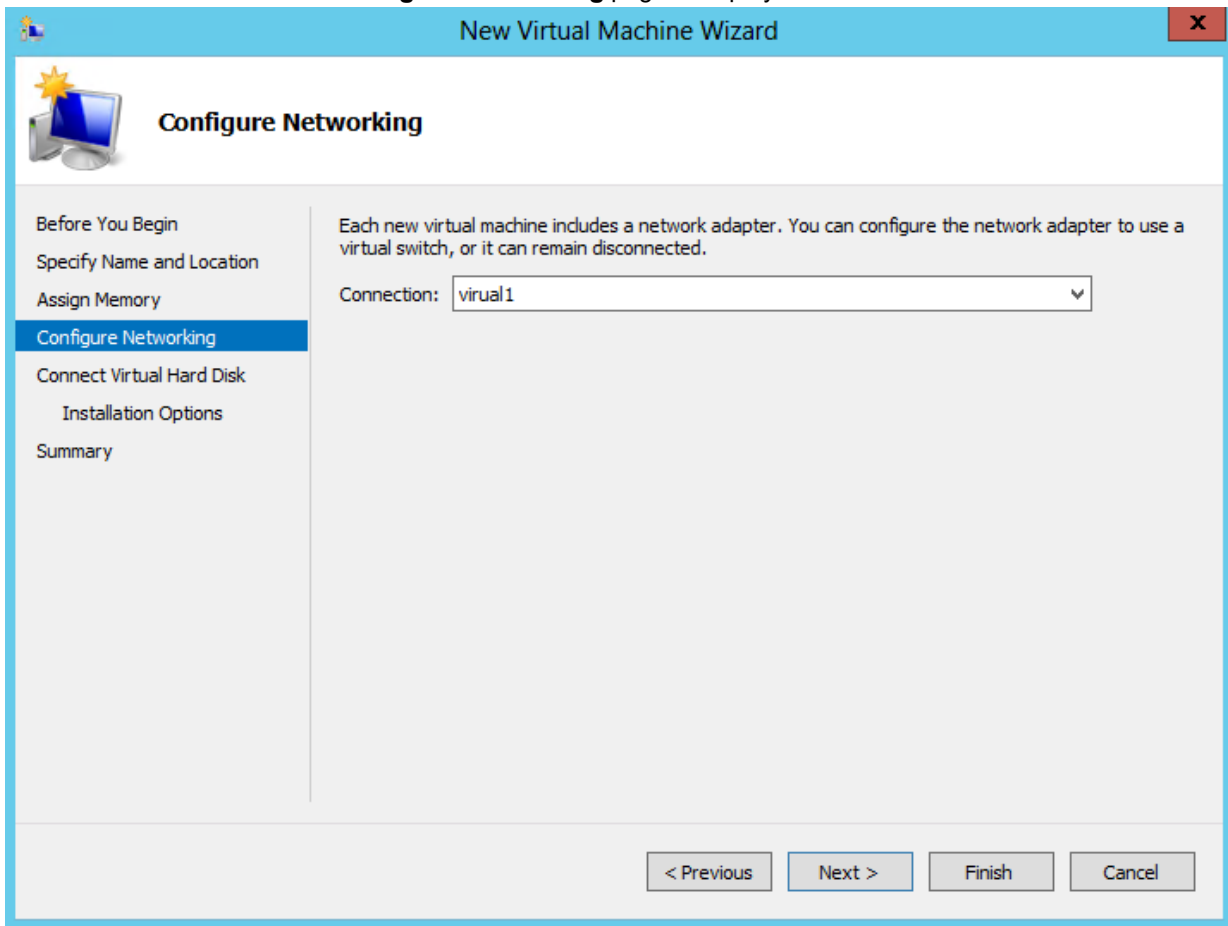
☐ Use Dynamic Memory for this virtual machine.

 When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

< Previous Next > Finish Cancel

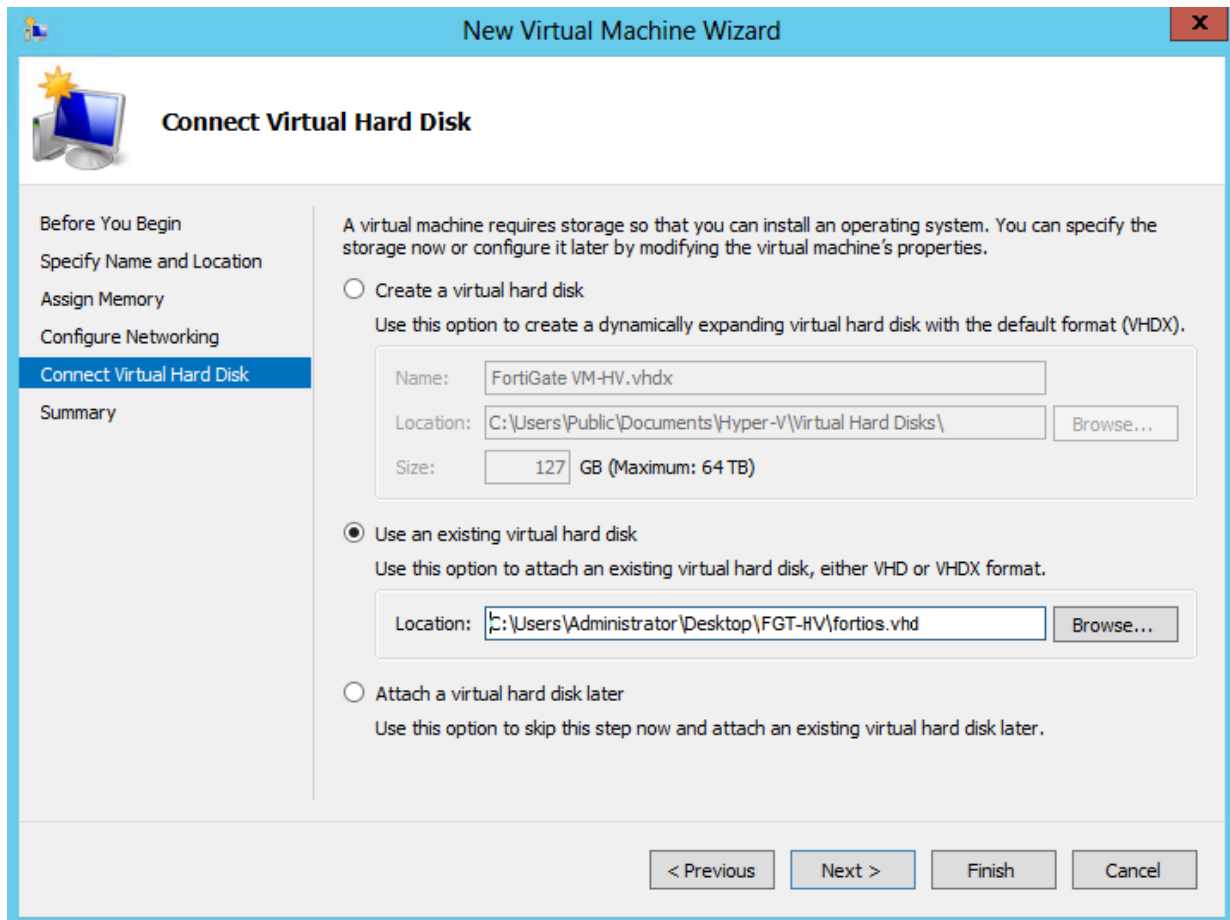
- Specify the amount of memory to allocate to this virtual machine. The default memory for FortiGate VM is 1GB (1024MB).

Select **Next** to continue. The **Configure Networking** page is displayed.



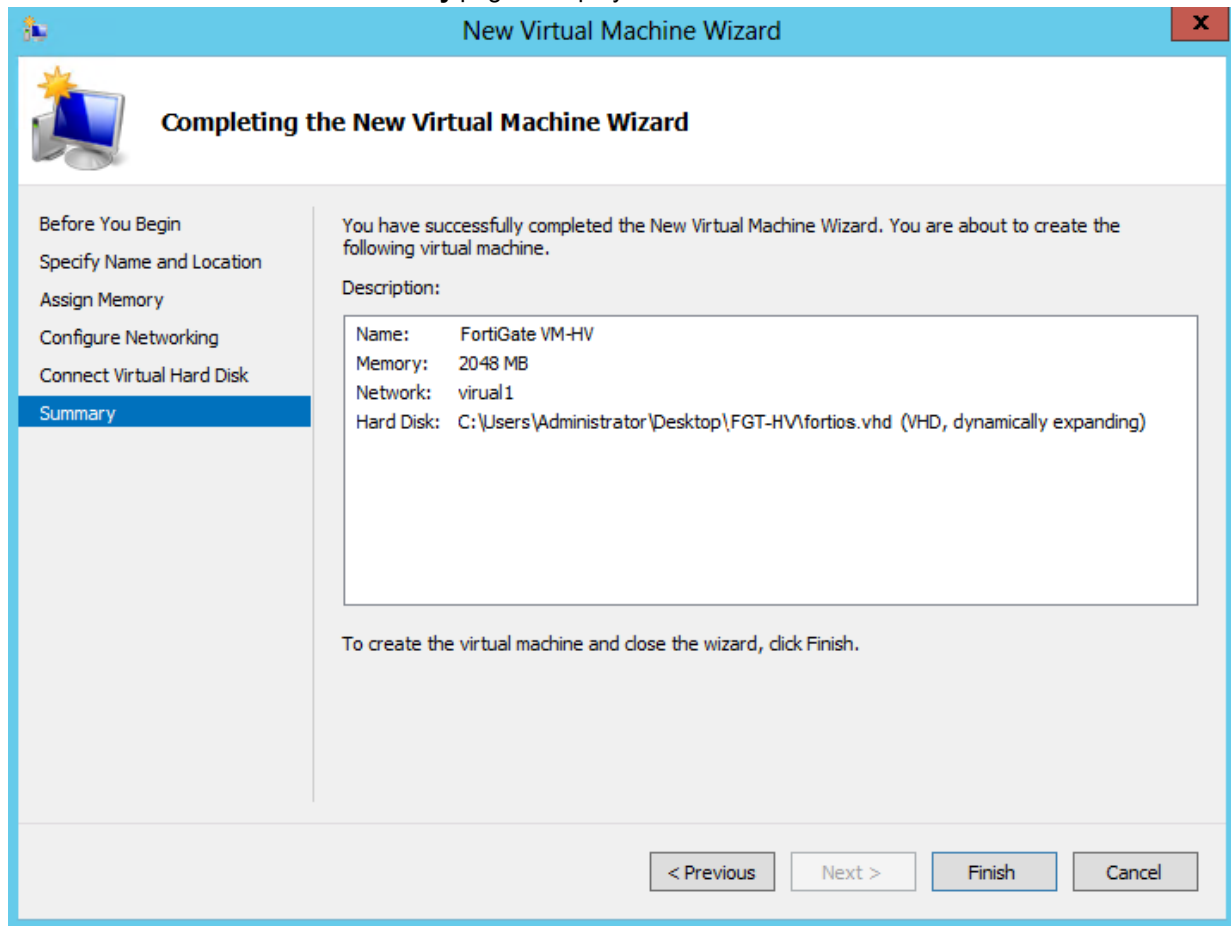
- Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. FortiGate VM requires four network adapters. You must configure network adapters in the **Settings** page.

Select **Next** to continue. The **Connect Virtual Hard Disk** page is displayed.



8. Select to use an existing virtual hard disk and browse for the `fortios.vhd` file that you downloaded from the [Fortinet Customer Service & Support portal](#).

Select **Next** to continue. The **Summary** page is displayed.



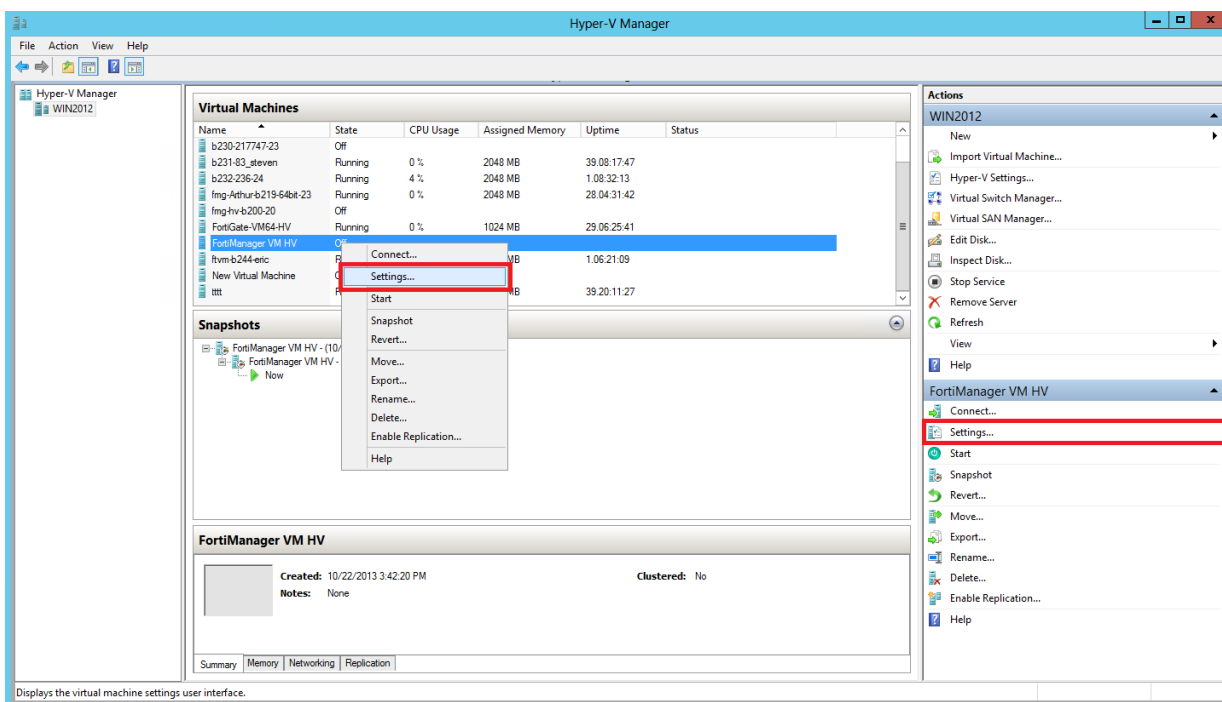
9. To create the virtual machine and close the wizard, select **Finish**.

Configure FortiGate VM hardware settings

Before powering on your FortiGate VM you must configure the virtual memory, virtual CPU, and virtual disk configuration to match your FortiGate VM license.

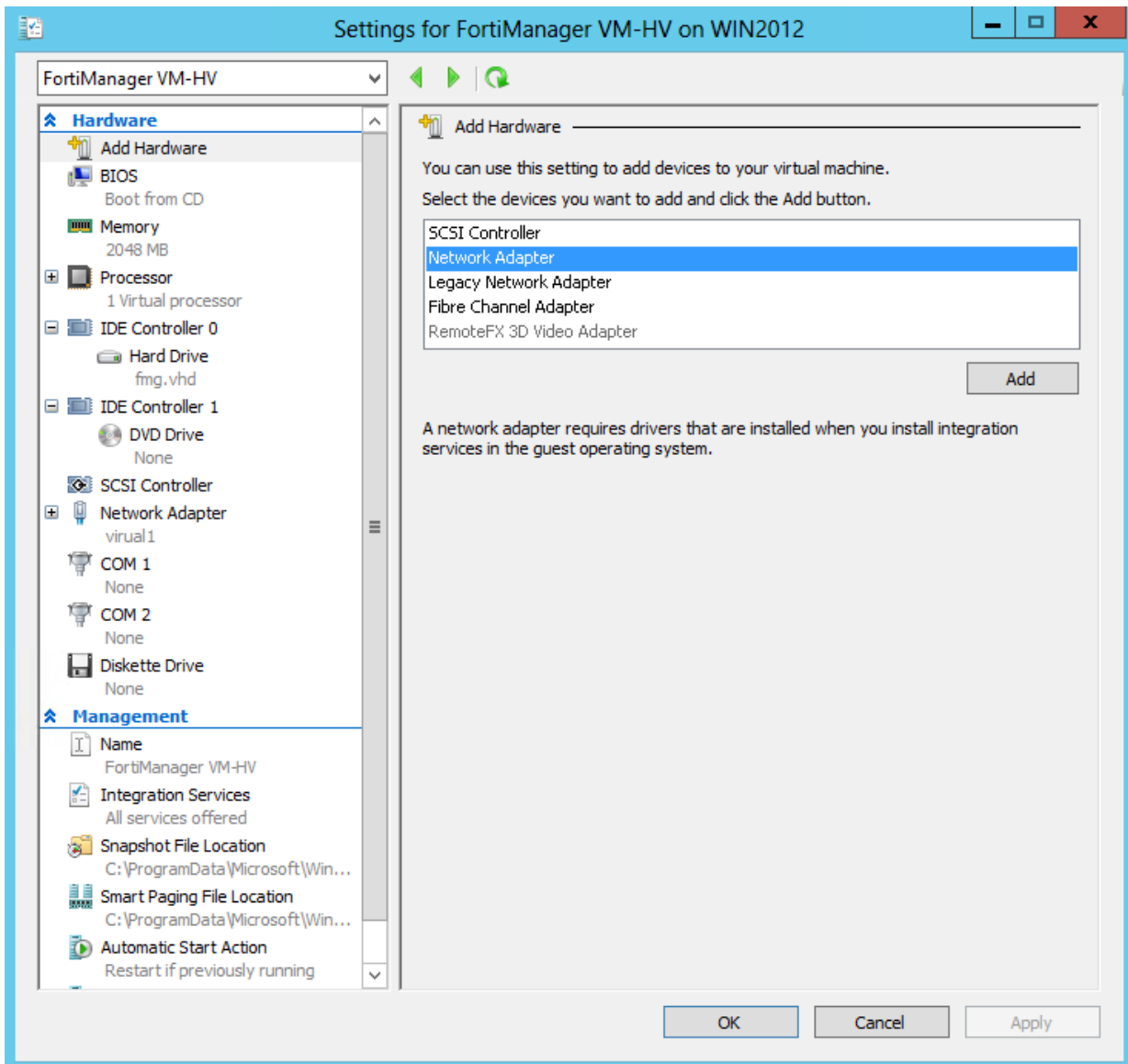
To configure settings for FortiGate VM on the server:

1. In the Hyper-V Manager, locate the name of the virtual machine, right-click the entry, and select **Settings** from the menu. Optionally, you can select the virtual machine and select **Settings** in the **Actions** menu.



Displays the virtual machine settings user interface.

The **Settings** page is displayed.



2. Configure virtual processors, network adapters, and virtual hard drive settings.
3. Select **Apply** to save the settings and then select **OK** to close the settings page.

FortiGate VM virtual processors

You must configure FortiGate VM virtual processors in the server settings page. The number of processors is dependent on your server environment.

Configure FortiGate VM virtual processors:

1. In the **Settings** page, select **Processor** from the **Hardware** menu.

The **Processor** page is displayed.

Processor

You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors:

Resource control

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage):	<input type="text" value="0"/>
Percent of total system resources:	<input type="text" value="0"/>
Virtual machine limit (percentage):	<input type="text" value="100"/>
Percent of total system resources:	<input type="text" value="75"/>
Relative weight:	<input type="text" value="100"/>

2. Configure the number of virtual processors for the FortiGate VM virtual machine. Optionally, you can use resource controls to balance resources among virtual machines.
3. Select **Apply** to save the settings.

FortiGate VM network adapters

You must configure FortiGate VM network adapters in the server settings page. FortiGate VM supports four network adapters.

Configure FortiGate VM network adapters:

1. In the **Settings** page, select **Add Hardware** from the **Hardware** menu, select **Network Adapter** in the device list, and select the **Add** button.

The **Network Adapter** page is displayed.

The screenshot shows the 'Network Adapter' configuration page. At the top, it says 'Specify the configuration of the network adapter or remove the network adapter.' Below this, there is a 'Virtual switch:' dropdown menu with 'Broadcom NetXtreme Gigabit Ethernet - Virtual Switch' selected. Under the 'VLAN ID' section, there is a checkbox for 'Enable virtual LAN identification' which is unchecked. Below the checkbox, a text box contains the value '2'. The 'Bandwidth Management' section also has an unchecked checkbox for 'Enable bandwidth management'. Below this, there are two rows for 'Minimum bandwidth:' and 'Maximum bandwidth:', each with a text box containing '0' and the unit 'Mbps'. A note at the bottom of this section says 'To leave the minimum or maximum unrestricted, specify 0 as the value.' At the bottom of the page, there is a 'Remove' button and a note: 'To remove the network adapter from this virtual machine, click Remove.' A final note at the very bottom says 'Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.'

1. You must manually configure four network adapters for FortiGate VM in the settings page. For each network adapter, select the virtual switch from the drop-down list.
2. Select **Apply** to save the settings.

FortiGate VM virtual hard disk


You must configure the FortiGate VM virtual hard disk in the server settings page.

If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

Configure a FortiGate VM virtual hard drive:

1. In the **Settings** page, select **IDE Controller 0 > Hard Drive** from the **Hardware** menu.

The **Hard Drive** page is displayed.

 **Hard Drive**

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.


Controller: Location:

Media

You can compact or convert a virtual hard disk by editing the associated file. Specify the full path to the file.

☒ Virtual hard disk:

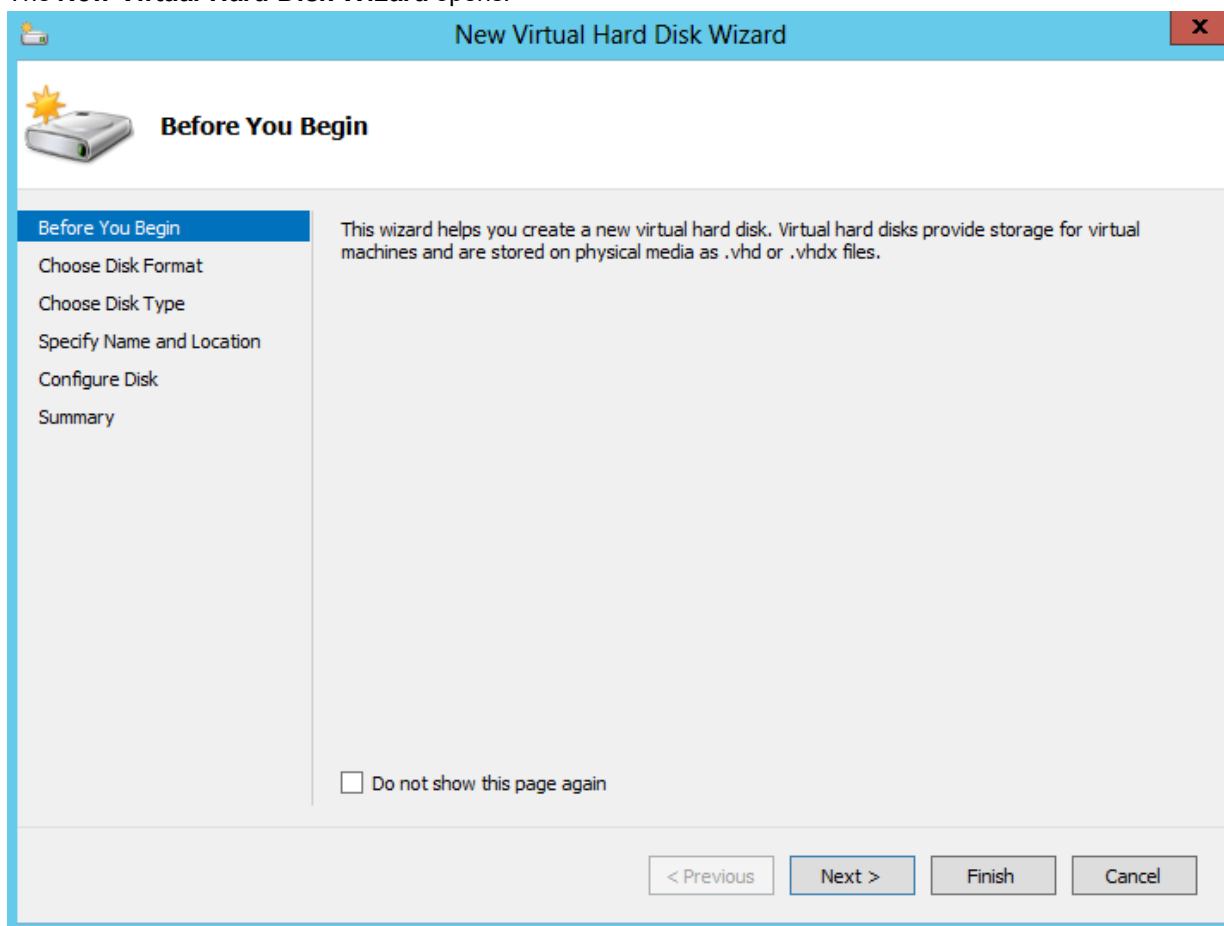
☐ Physical hard disk:

 If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

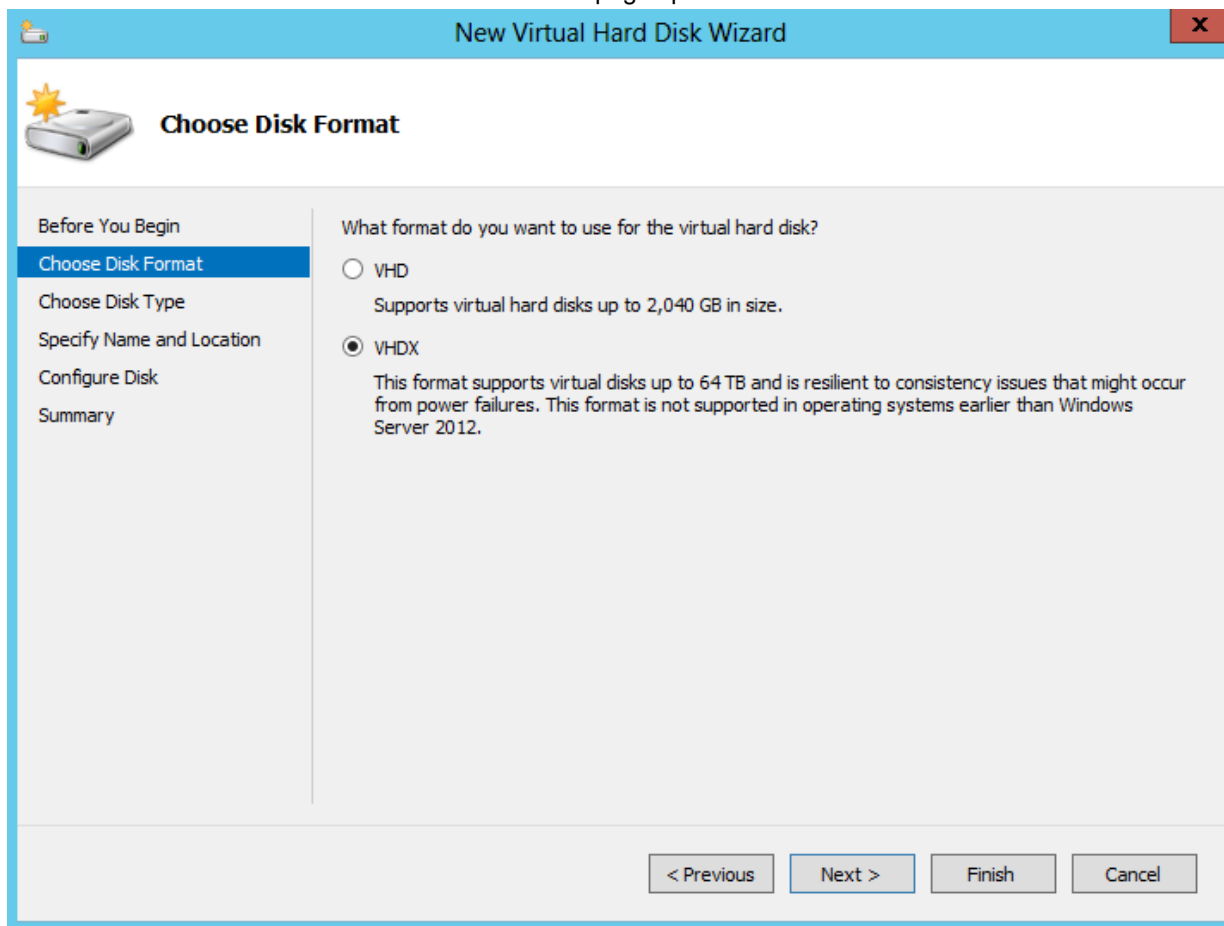
2. Select **New** to create a new virtual hard disk.

The **New Virtual Hard Disk Wizard** opens.



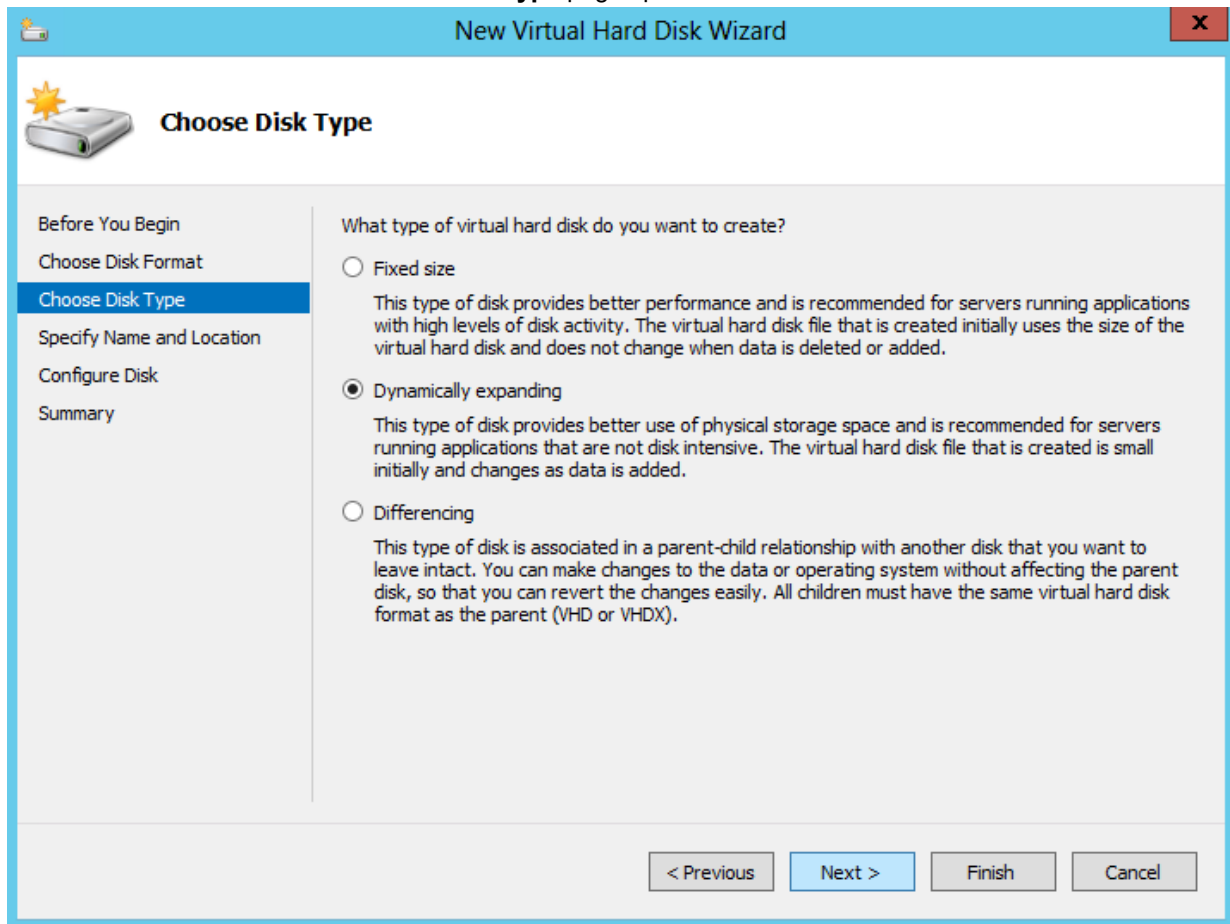
3. This wizard helps you to create a new virtual hard disk.

Select **Next** to continue. The **Choose Disk Format** page opens.



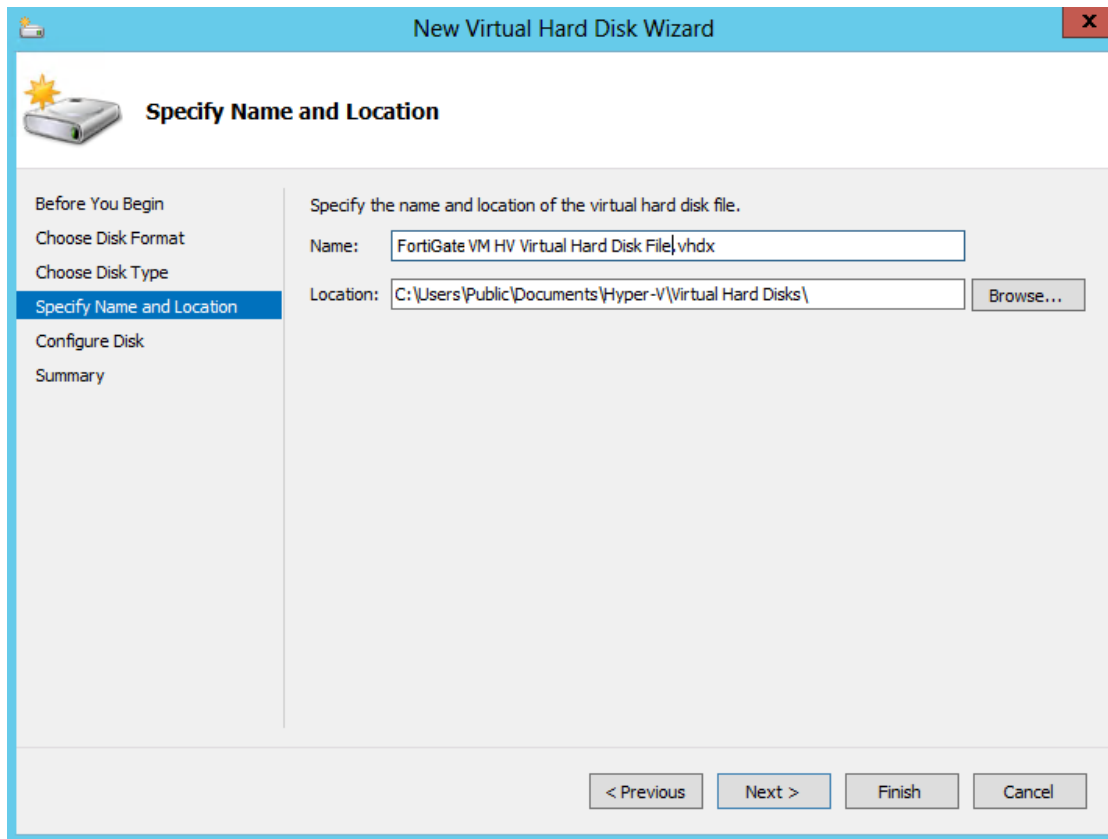
4. Select to use VHDX format virtual hard disks. This format supports virtual disks up to 64TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012. Note that FortiGate-VM does not support hard disks larger than 2TB.

Select **Next** to continue. The **Choose Disk Type** page opens.



5. Select the type of virtual disk you want to use. Select one of the following disk types:
- **Fixed size:** This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.
 - **Dynamic expanding:** This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual disk file that is created is small initially and changes as data is added.
 - **Differencing:** This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

Select **Next** to continue. The **Specify Name and Location** page opens.



6. Specify the name and location of the virtual hard disk file. Use the **Browse** button to select a specific file folder on your server.

Select **Next** to continue. The **Configure Disk** page opens.

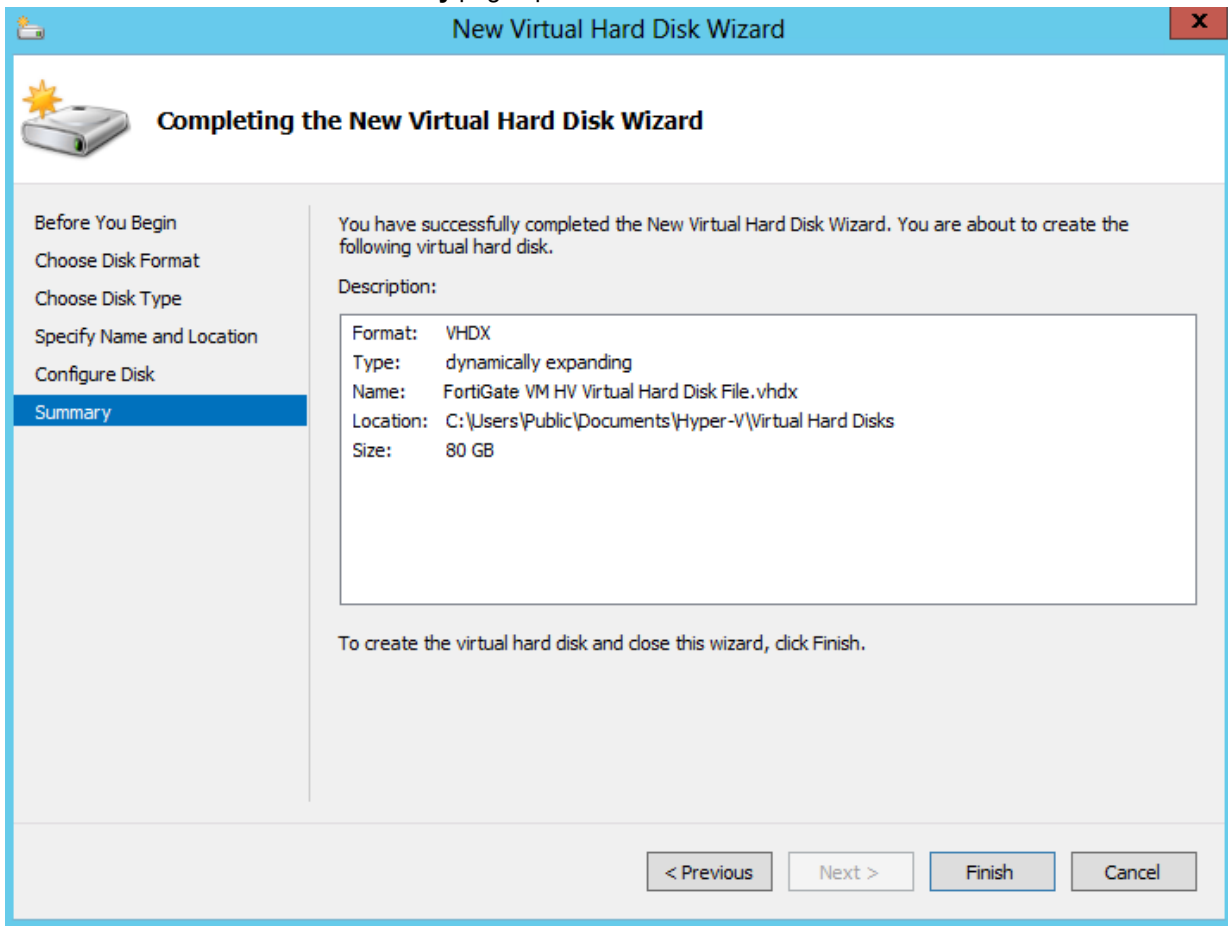
The screenshot shows the 'New Virtual Hard Disk Wizard' window with the 'Configure Disk' step selected. The left sidebar contains the following steps: 'Before You Begin', 'Choose Disk Format', 'Choose Disk Type', 'Specify Name and Location', 'Configure Disk' (highlighted), and 'Summary'. The main area has a heading 'Configure Disk' with a disk icon. Below it, a message states: 'You can create a blank virtual hard disk or copy the contents of an existing physical disk.' There are two radio button options: 'Create a new blank virtual hard disk' (selected) and 'Copy the contents of the specified physical disk:'. The 'Create a new blank virtual hard disk' option has a 'Size:' field set to '30' GB (Maximum: 64 TB). The 'Copy the contents of the specified physical disk:' option has a table listing physical drives:

Physical Hard Disk	Size
\\.\PHYSICALDRIVE0	1863 GB
\\.\PHYSICALDRIVE1	125 MB
\\.\PHYSICALDRIVE2	125 MB
\\.\PHYSICALDRIVE3	125 MB
\\.\PHYSICALDRIVE4	125 MB

Below the table, there is another radio button option: 'Copy the contents of the specified virtual hard disk'. This option has a 'Path:' field and a 'Browse...' button. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

7. Select to **Create a new blank virtual hard disk** and enter the size of the disk in GB. The maximum size is dependent on your server environment.

Select **Next** to continue. The **Summary** page opens.



8. The summary page provides details of the virtual hard disk. Select **Finish** to create the virtual hard disk.
9. Select **Apply** to save the settings and select **OK** to exit the settings page.

High Availability Hyper-V configuration

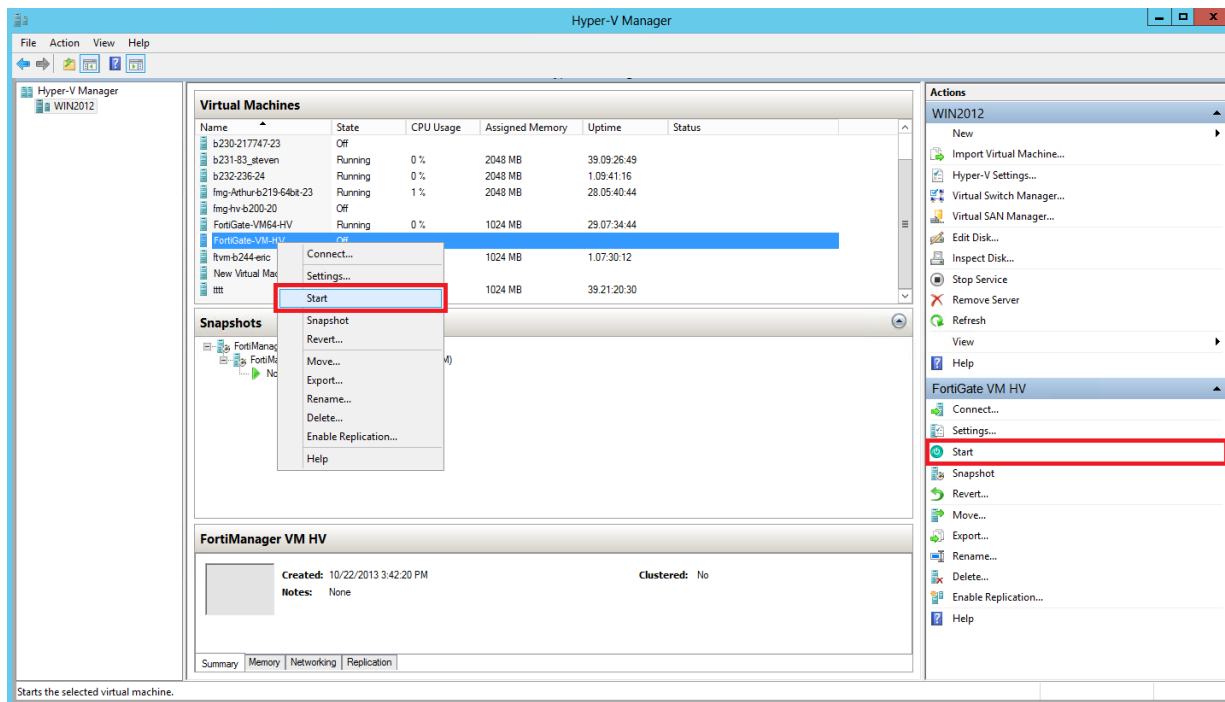
Promiscuous mode and support for MAC address spoofing is required for FortiGate-VM for Hyper-V to support FortiGate Clustering Protocol (FGCP) high availability (HA). By default the FortiGate-VM for Hyper-V has promiscuous mode enabled in the XML configuration file in the FortiGate-VM Hyper-V image. If you have problems with HA mode, confirm that this is still enabled.

In addition, because the FGCP applies virtual MAC addresses to FortiGate data interfaces and because these virtual MAC addresses mean that matching interfaces of different FortiGate-VM instances will have the same virtual MAC addresses you have to configure Hyper-V to allow MAC spoofing. But you should only enable MAC spoofing for FortiGate-VM data interfaces. You should not enable MAC spoofing for FortiGate HA heartbeat interfaces.

With promiscuous mode enabled and the correct MAC spoofing settings you should be able to configure HA between two or more FortiGate-VM for Hyper-V instances.

Start the FortiGate VM

You can now proceed to power on your FortiGate VM. Select the name of the FortiGate VM in the list of virtual machines, right-click, and select **Start** in the menu. Optionally, you can select the name of the FortiGate VM in the list of virtual machines and select **Start** in the **Actions** menu.



Deployment example – KVM

Once you have downloaded the FORTINET.out.kvm.zip file and extracted virtual hard drive image file fortios.qcow2, you can create the virtual machine in your KVM environment.

The following topics are included in this section:

- [Create the FortiGate VM virtual machine](#)
- [Configure FortiGate VM hardware settings](#)
- [Start the FortiGate VM](#)

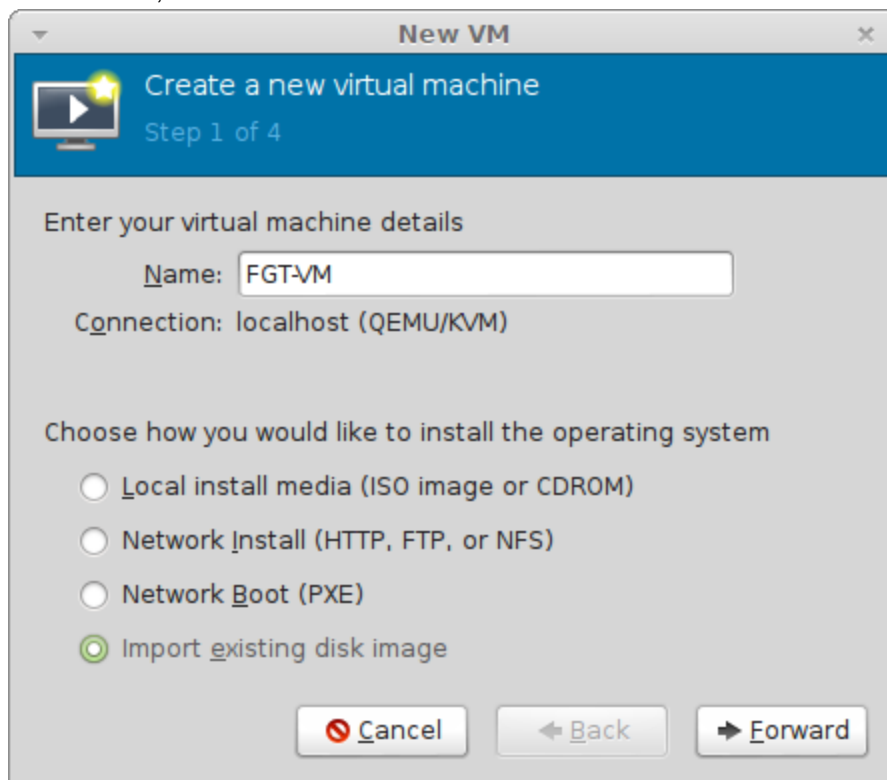
Create the FortiGate VM virtual machine

To create the FortiGate VM virtual machine:

1. Launch Virtual Machine Manager (virt-manager) on your KVM host server.

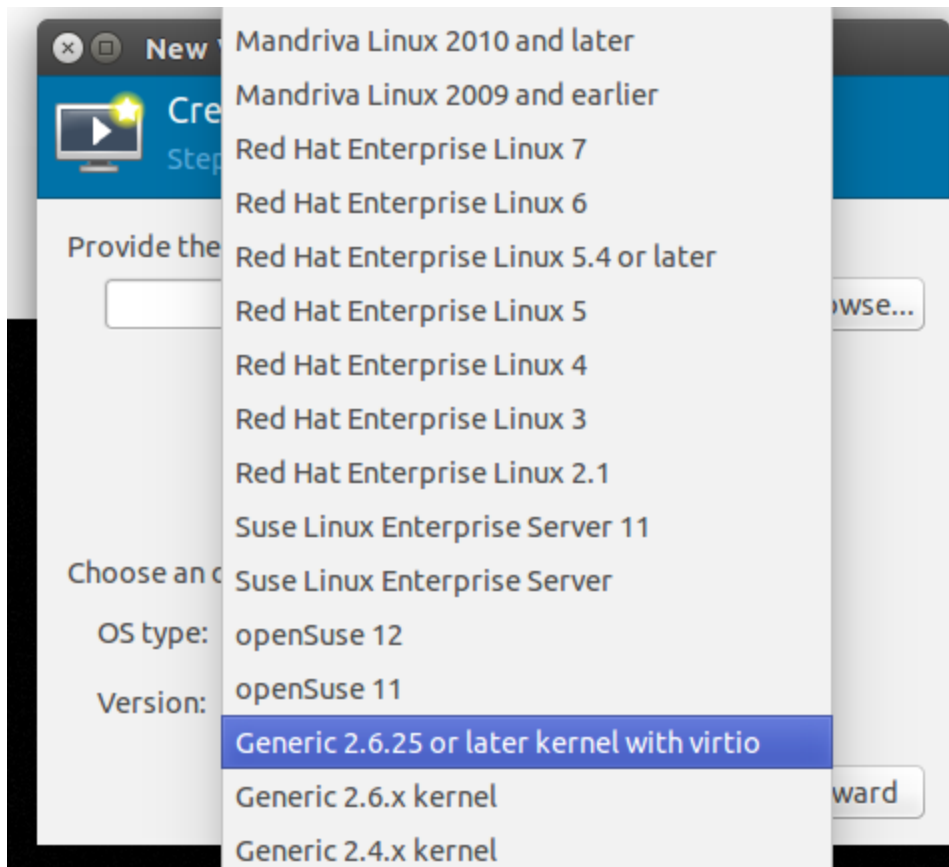
The **Virtual Machine Manager** home page opens.

2. In the toolbar, select **Create a new virtual machine**.



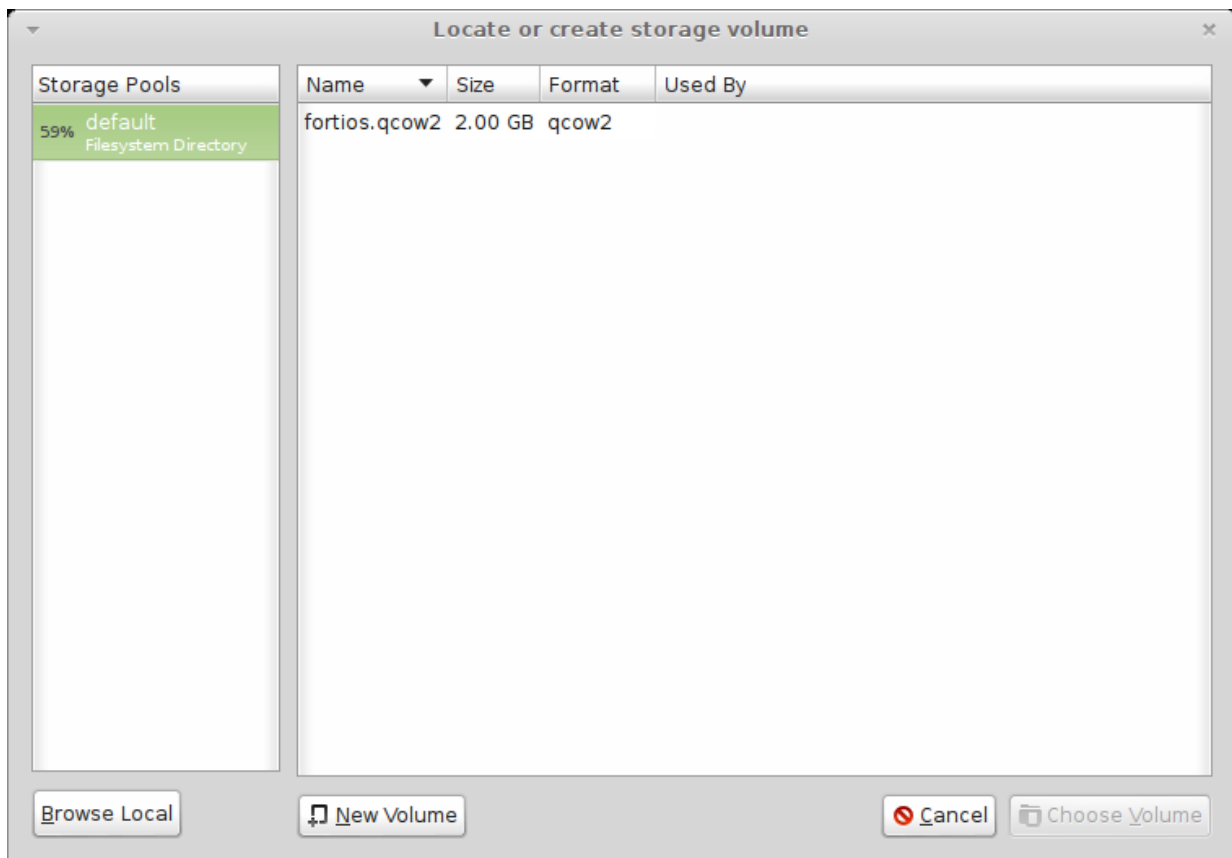
3. Enter a **Name** for the VM, FGT-VM for example.
4. Ensure that **Connection** is localhost. (This is the default.)
5. Select **Import existing disk image**.

6. Select **Forward**.



7. In **OS Type** select **Linux**.

8. In **Version**, select a Generic version with virtio.

9. Select **Browse**.

10. If you copied the fortios.qcow2 file to `/var/lib/libvirt/images`, it will be visible on the right. If you saved it somewhere else on your server, select **Browse Local** and find it.
11. Choose **Choose Volume**.
12. Select **Forward**.
13. Specify the amount of memory and number of CPUs to allocate to this virtual machine. The amounts must not exceed your license limits. See [FortiGate VM Overview on page 10](#).
14. Select **Forward**.
15. Expand **Advanced options**. A new virtual machine includes one network adapter by default. Select a network adapter on the host computer. Optionally, set a specific MAC address for the virtual network interface. Set **Virt Type** to **virtio** and **Architecture** to **qcow2**.
16. Select **Finish**.

Configure FortiGate VM hardware settings

Before powering on your FortiGate VM you must add the log disk and configure the virtual hardware of your FortiGate VM.

To configure settings for FortiGate VM on the server:

1. In the Virtual Machine Manager, locate the name of the virtual machine and then select **Open** from the toolbar.
2. Select **Add Hardware**. In the **Add Hardware** window select **Storage**.

3. Select **Create a disk image on the computer's harddrive** and set the size to 30GB.



If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

4. Enter:

Device type	Virtio disk
Cache mode	Default
Storage format	raw



Even though raw is the storage format listed, the qcow2 format is also supported.

5. Select **Network** to configure add more the network interfaces. The **Device type** must be **Virtio**.

A new virtual machine includes one network adapter by default. You can add more through the Add Hardware window. FortiGate VM requires four network adapters. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.

6. Select **Finish**.

Start the FortiGate VM

You can now proceed to power on your FortiGate VM. Select the name of the FortiGate VM in the list of virtual machines. In the toolbar, select **Console** and then select **Start**.

Deployment example – OpenXen

Once you have downloaded the FORTINET.out.OpenXen.zip file and extracted virtual hard drive image file fortios.qcow2, you can create the virtual machine in your OpenXen environment.

The following topics are included in this section:

[Create the FortiGate VM virtual machine \(VMM\)](#)

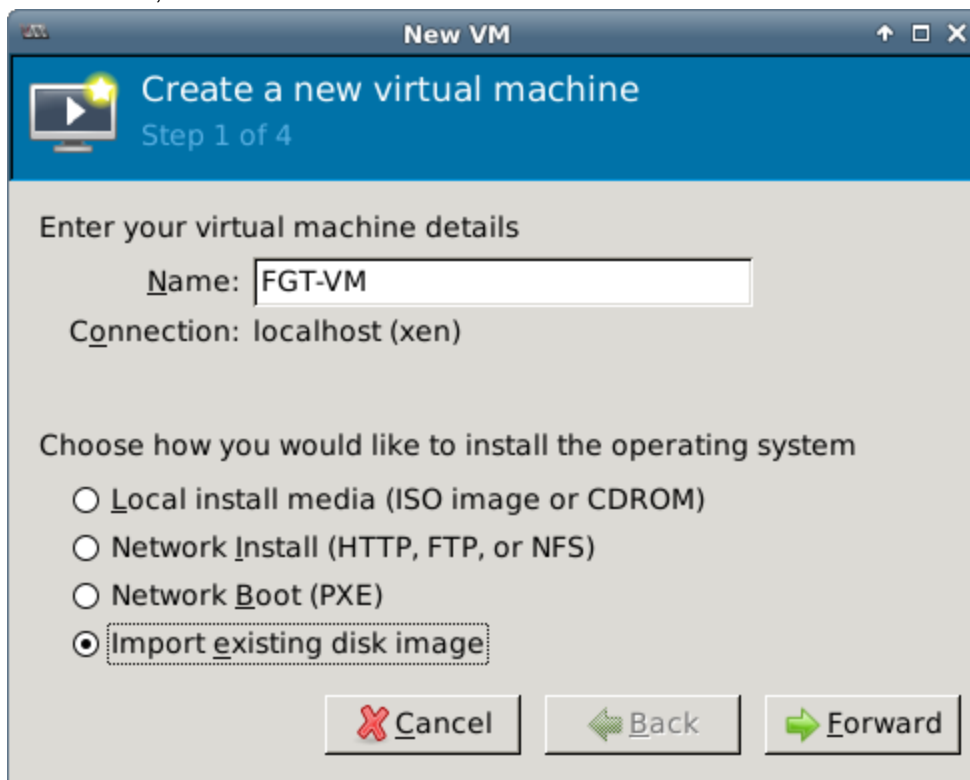
Create the FortiGate VM virtual machine (VMM)

To create the FortiGate VM virtual machine:

1. Launch Virtual Machine Manager (virt-manager) on your OpenXen host server.

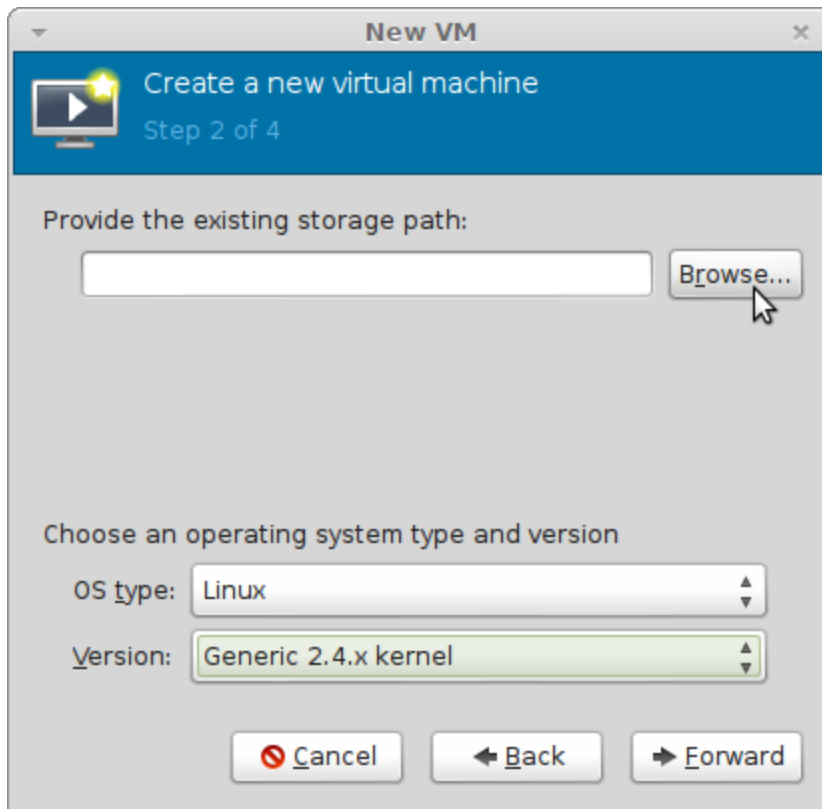
The **Virtual Machine Manager** home page opens.

2. In the toolbar, select **Create a new virtual machine**.



3. Enter a **Name** for the VM, FGT-VM for example.
4. Ensure that **Connection** is localhost. (This is the default.)
5. Select **Import existing disk image**.

6. Select **Forward**.



7. In **OS Type** select **Linux**.

8. In **Version**, select **Generic 2.4.x.kernel**.

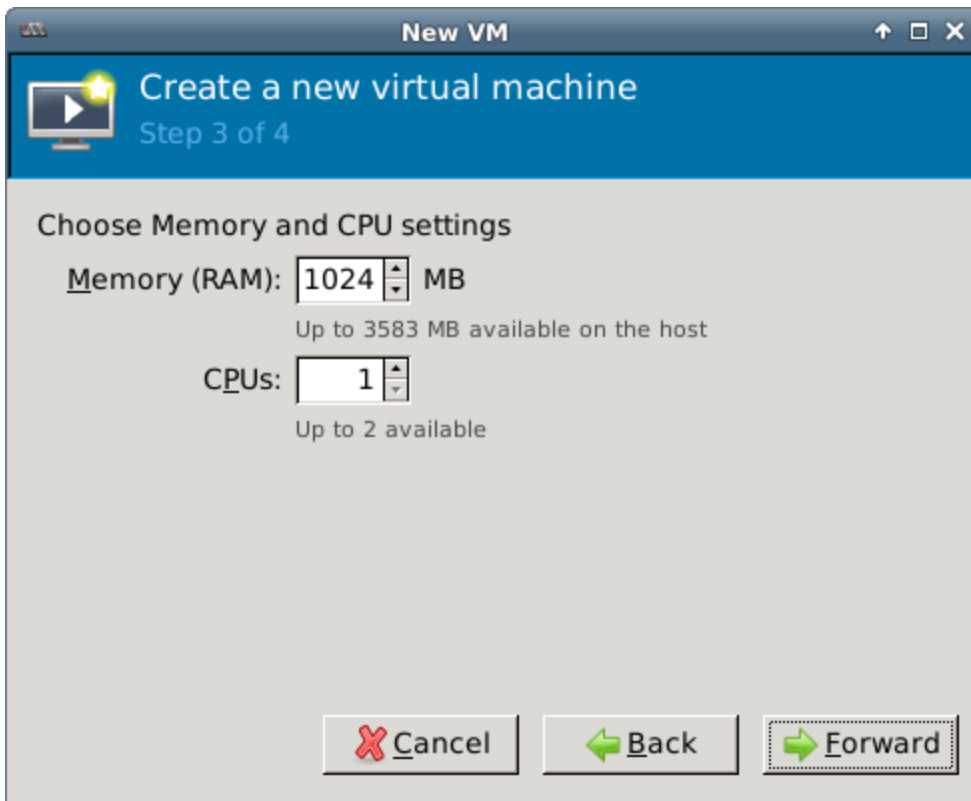
9. Select **Browse**.

The **Locate or create storage volume** window opens.

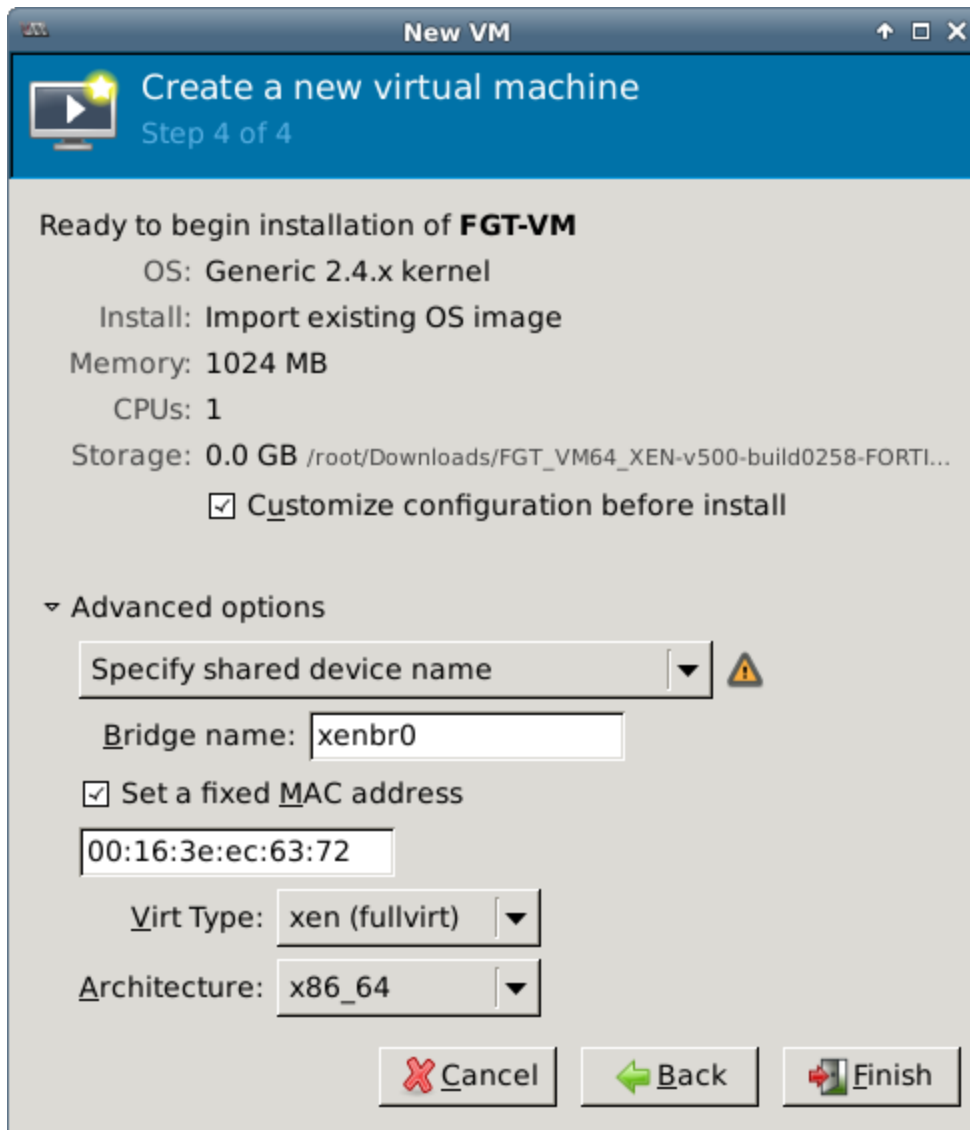
10. Select **Browse Local**, find the fortios.qcow2 disk image file.

11. Select fortios.qcow2 and select **Choose Volume**.

12. Select **Forward**.

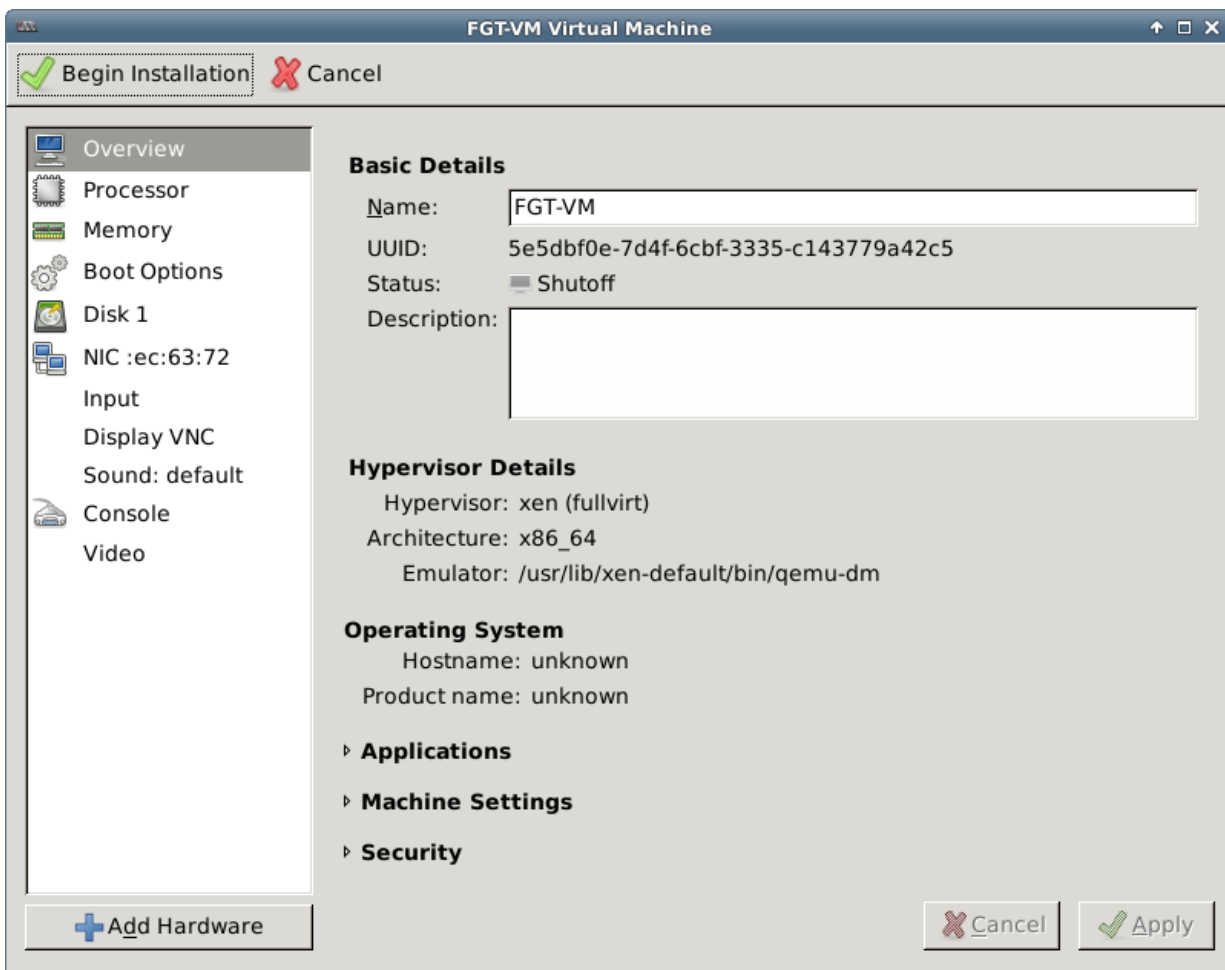


13. Specify the amount of memory and number of CPUs to allocate to this virtual machine. The amounts must not exceed your license limits.

14. Select Forward.

- 15. Select **Customize configuration before install**.** This enables you to make some hardware configuration changes before VM creation is started.
- 16. Expand **Advanced options**.** A new virtual machine includes one network adapter by default. Select **Specify shared device name** and enter the name of the bridge interface on the OpenXen host. Optionally, set a specific MAC address for the virtual network interface. **Virt Type** and **Architecture** are set by default and should be correct.
- 17. Select **Finish**.**

The virtual machine hardware configuration window opens.



You can use this window to add hardware such as network interfaces and disk drives.

18. Select **Add Hardware**. In the **Add Hardware** window select **Storage**.
19. Select **Create a disk image on the computer's hddrive** and set the size to 30GB.



If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30GB. The VM license limit is 2TB.

20. Enter:

Device type	Virtio disk
Cache mode	Default
Storage format	raw

21. Select **Network** to configure add more the network interfaces. The **Device type** must be **Virtio**.

A new virtual machine includes one network adapter by default. You can add more through the Add Hardware window. FortiGate VM requires four network adapters. You can configure network adapters to connect to a virtual

switch or to network adapters on the host computer.

22. Select **Finish.**

23. Select **Begin Installation.** After the installation completes successfully, the VM starts and the console window opens.

Deployment example – Citrix XenServer

Once you have downloaded the FORTINET.out.CitrixXen.zip file and extracted the files, you can create the virtual machine in your Citrix Xen environment.

The following topics are included in this section:

[Create the FortiGate VM virtual machine \(XenCenter\)](#)

[Configure virtual hardware](#)

Create the FortiGate VM virtual machine (XenCenter)

To create the FortiGate VM virtual machine from the OVF file

1. Launch XenCenter on your management computer.

The management computer can be any computer that can run Citrix XenCenter, a Windows application.

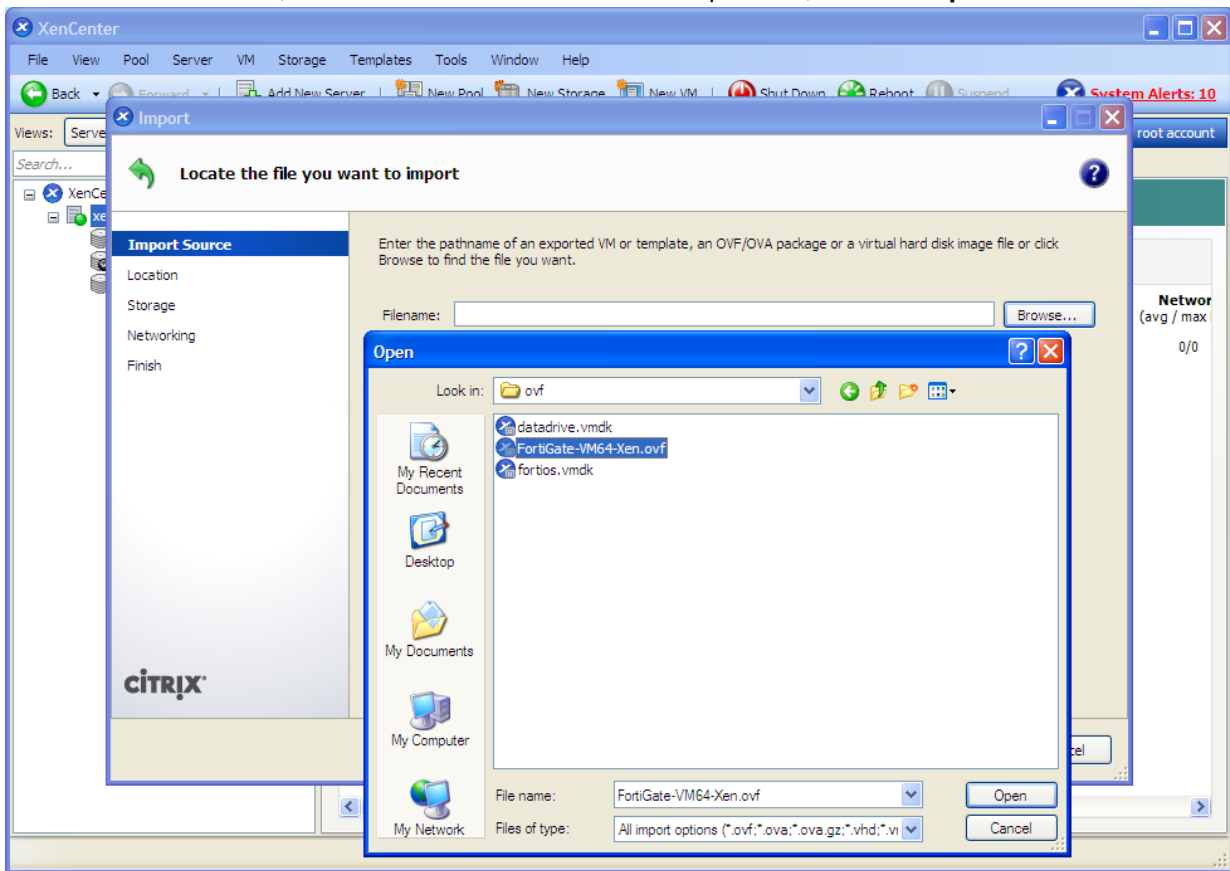
2. If you have not already done so, select **ADD a server**. Enter your Citrix XenServer IP address and the root logon credentials required to manage that server.

Your Citrix XenServer is added to the list in the left pane.

The **Virtual Machine Manager** home page opens.

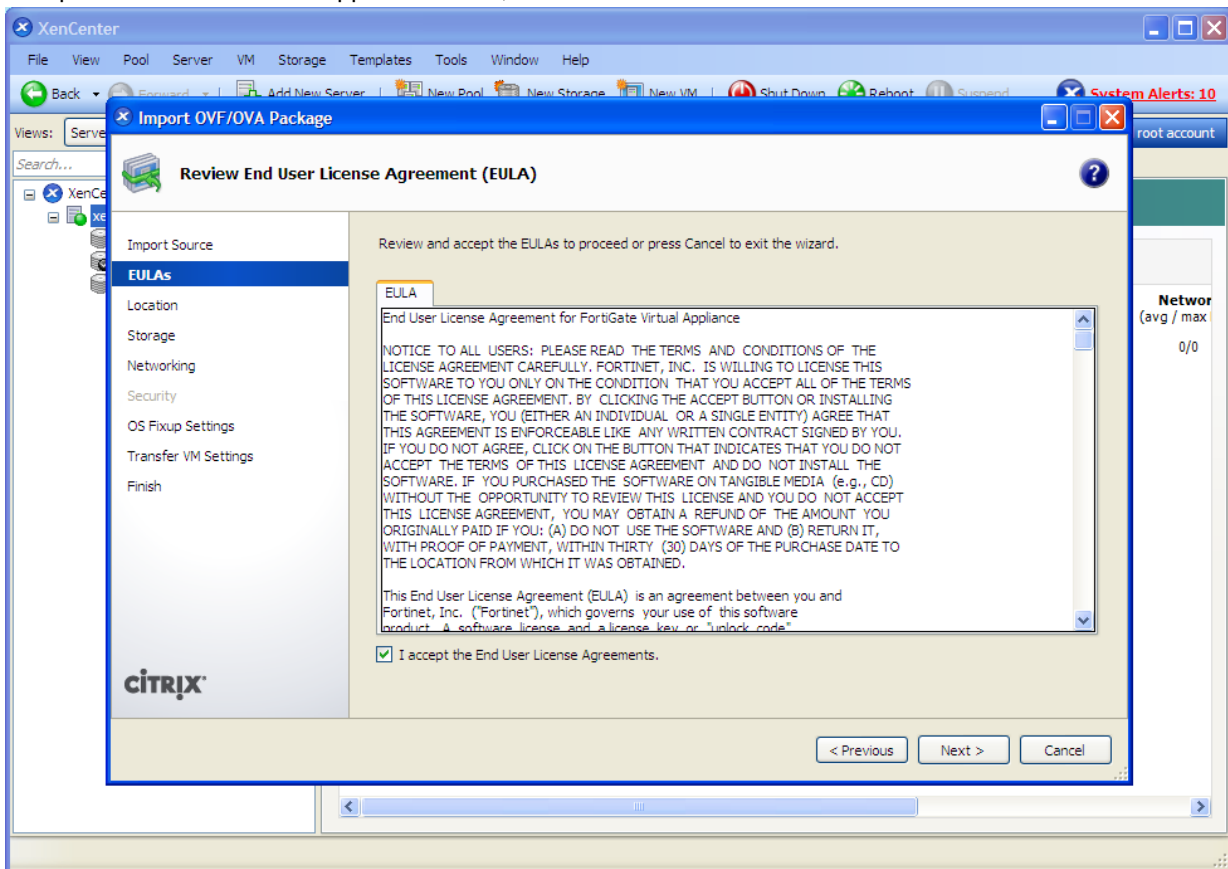
3. Go to **File > Import**. An import dialog will appear.

- Click the **Browse** button, find the FortiGate-VM64-Xen.ovf template file, then click **Open**.



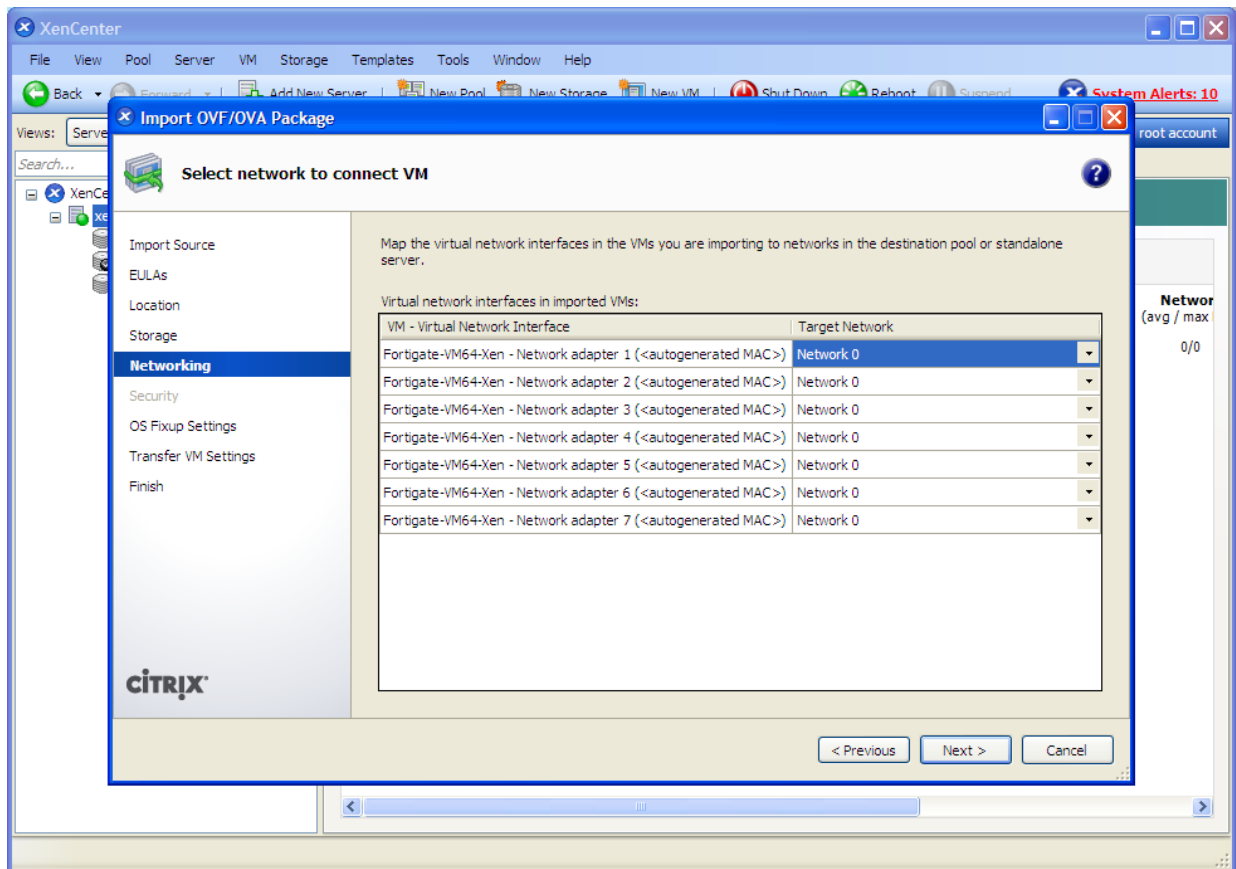
- Select **Next**.

6. Accept the FortiGate Virtual Appliance EULA, then select **Next**.



7. Choose the pool or standalone server that will host the VM, then select **Next**.
8. Select the storage location for FortiGate VM disk drives or accept the default. Select **Next**.

- Configure how each vNIC (virtual network adapter) in FortiGate VM will be mapped to each vNetwork on the Citrix XenServer, then click **Next**.



- Click **Next** to skip OS fixup.
- Select **Next** to use the default network settings for transferring the VM to the host.
- Select **Finish**.

The Citrix XenServer imports the FortiGate VM files and configures the VM as specified in the OVF template. Depending on your computer's hardware speed and resource load, and also on the file size and speed of the network connection, this might take several minutes to complete.



When VM import is complete, the XenCenter left pane includes the FortiGate VM in the list of deployed VMs for your Citrix XenServer.

Configure virtual hardware

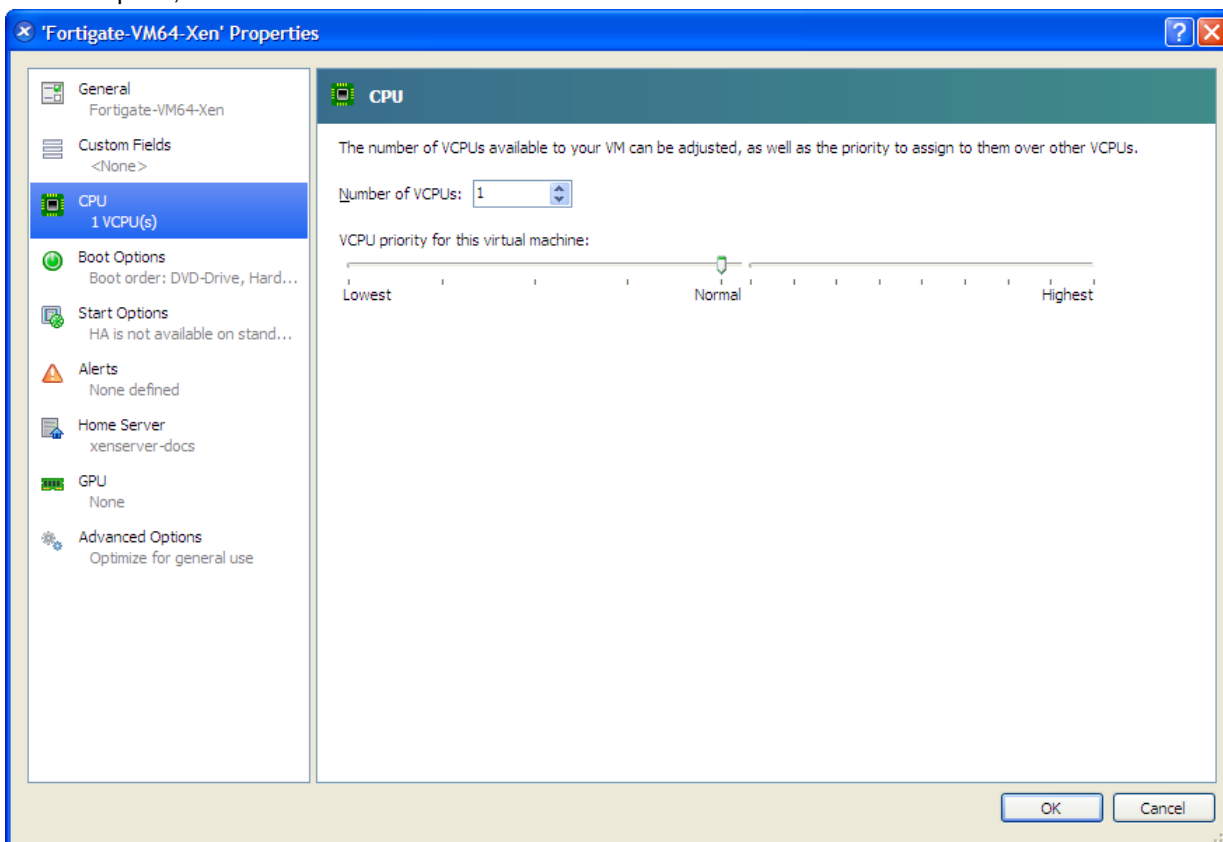
Before you start your FortiGate-VM for the first time, you need to adjust your virtual machine's virtual hardware settings to meet your network requirements.

Configuring number of CPUs and memory size

Your FortiGate-VM license limits the number CPUs and amount of memory that you can use. The amounts you allocate must not exceed your license limits.

To access virtual machine settings

1. Open XenCenter.
2. Select your FortiGate VM in the left pane.
The tabs in the right pane provide access to the virtual hardware configuration. The Console tab provides access to the FortiGate console.
1. To set the number of CPUs
2. In the XenCenter left pane, right-click the FortiGate VM and select Properties.
The Properties window opens.
3. In the left pane, select CPU.

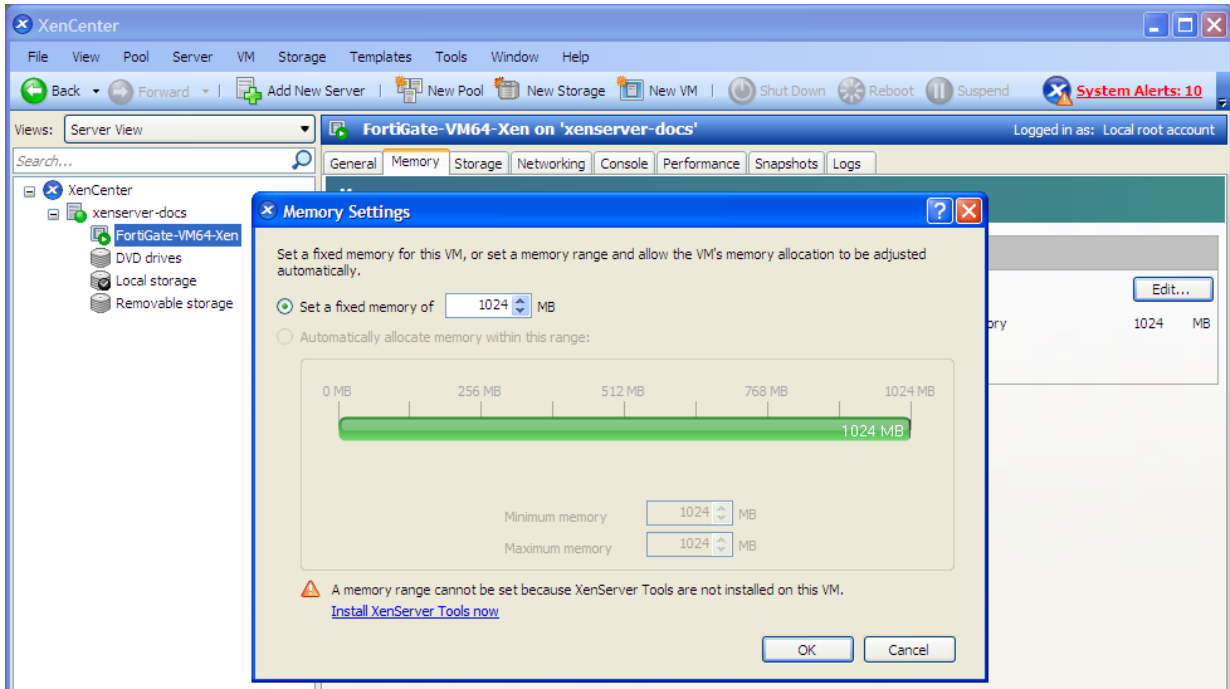


4. Adjust **Number of CPUs** and then select **OK**.

XenCenter will warn if you select more CPUs than the Xen host computer contains. Such a configuration might reduce performance.

To set memory size

1. In the XenCenter left pane, select the FortiGate VM.
2. In the right pane, select the **Memory** tab.
3. Select **Edit**, modify the value in the **Set a fixed memory of** field and select **OK**.



Configuring disk storage

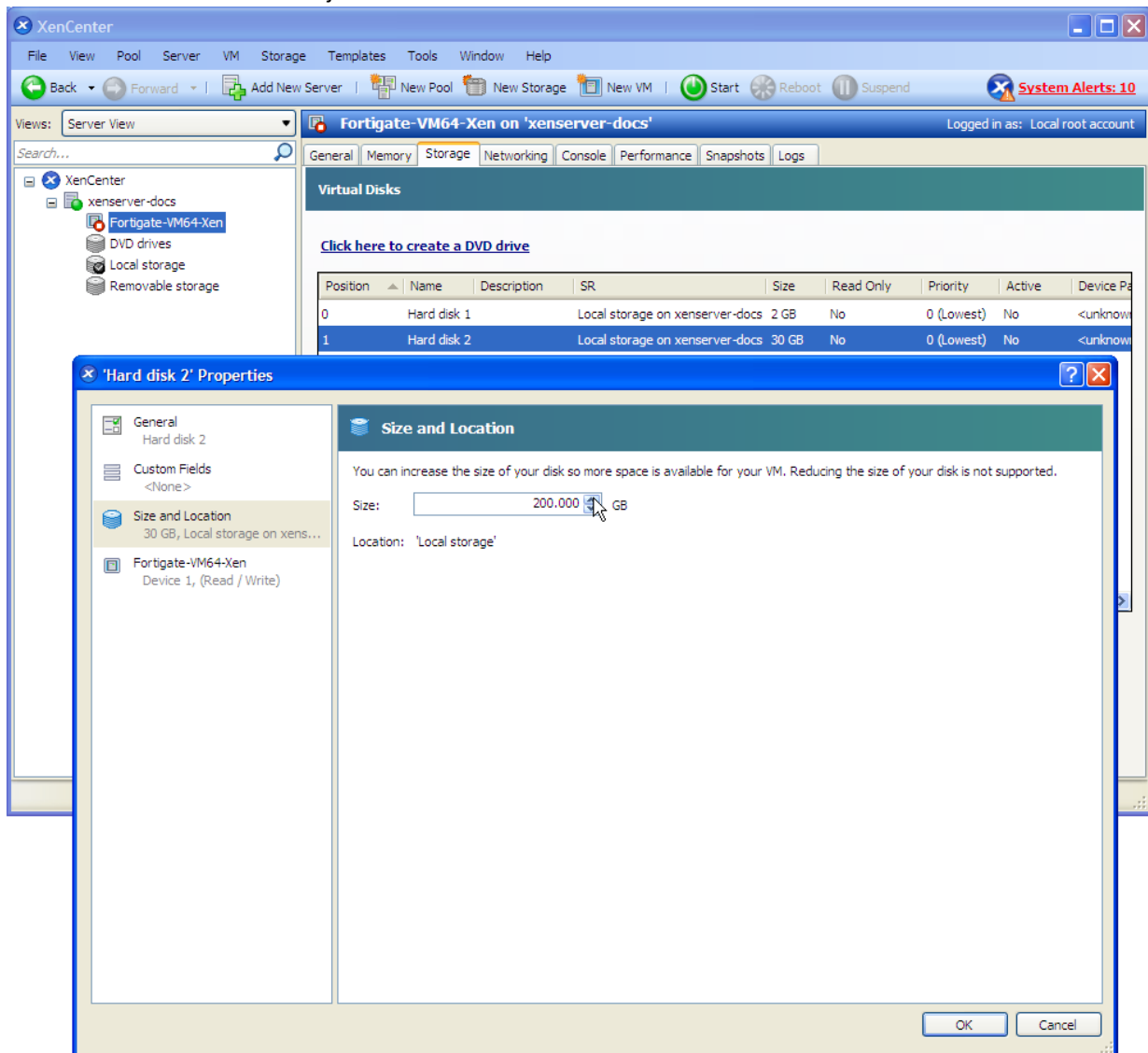
By default the FortiGate VM data disk 30GB. You will probably want to increase this. Disk resizing must be done before you start the VM for the first time.

To resize the FortiGate data disk

1. In the XenCenter left pane, select the FortiGate VM.
2. Select the **Storage** tab. Select **Hard disk 2** (the 30GB drive), then select **Properties**.

The '**Hard disk 2**' **Properties** window opens.

3. Select **Size and Location**. Adjust **Size** and select **OK**.



FortiGate VM Initial Configuration

Before you can connect to the FortiGate VM web-based manager you must configure a network interface in the FortiGate VM console. Once an interface with administrative access is configured, you can connect to the FortiGate VM web-based Manager and upload the FortiGate VM license file that you downloaded from the [Customer Service & Support](#) website.

The following topics are included in this section:

[Set FortiGate VM port1 IP address](#)

[Connect to the FortiGate VM Web-based Manager](#)

[Upload the FortiGate VM license file](#)

[Validate the FortiGate VM license with FortiManager](#)

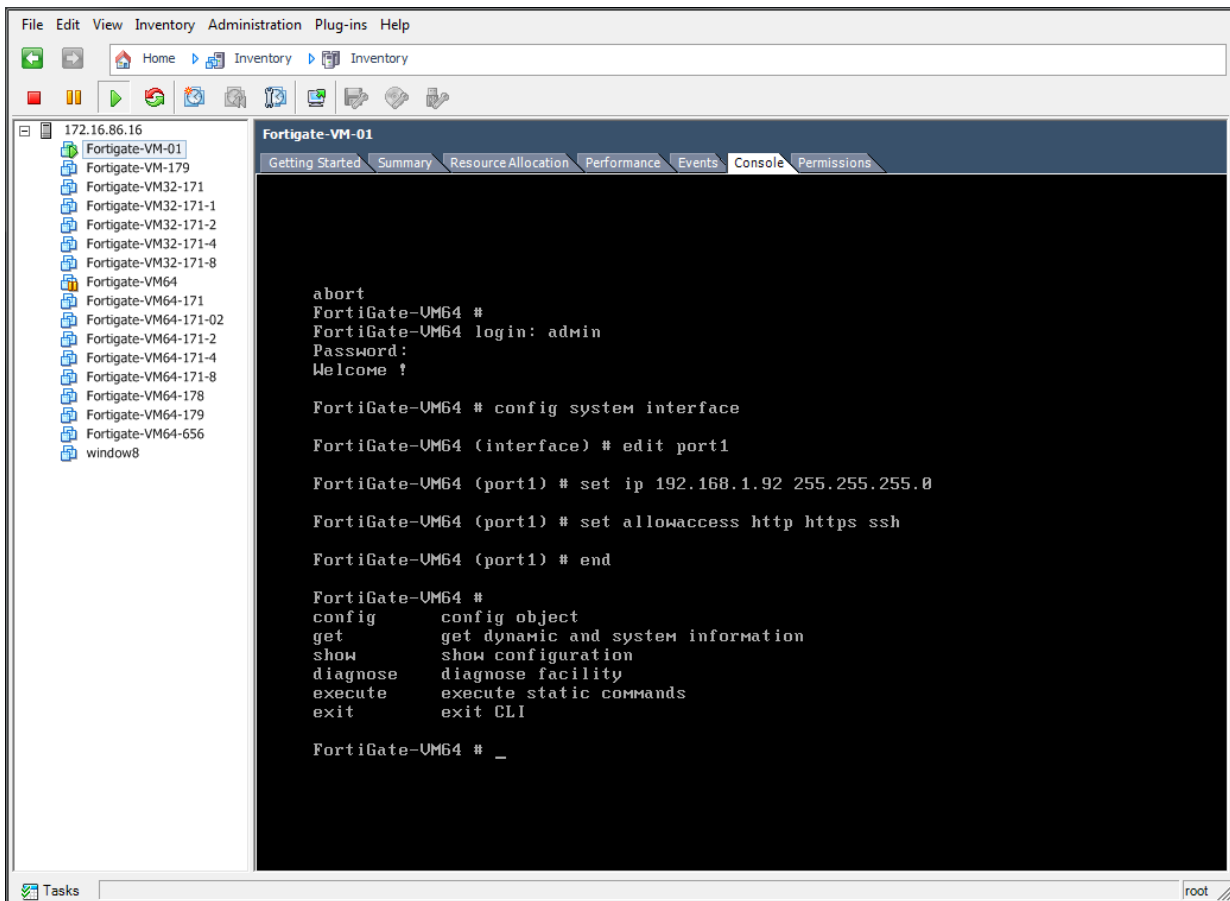
Set FortiGate VM port1 IP address

Hypervisor management environments include a guest console window. On the FortiGate VM, this provides access to the FortiGate console, equivalent to the console port on a hardware FortiGate unit. Before you can access the Web-based manager, you must configure FortiGate VM port1 with an IP address and administrative access.

To configure the port1 IP address:

1. In your hypervisor manager, start the FortiGate VM and access the console window. You might need to press Return to see a login prompt.

Example of FortiGate VM console access:



2. At the FortiGate VM login prompt enter the username `admin`. By default there is no password. Just press Return.
3. Using CLI commands, configure the port1 IP address and netmask. Also, HTTP access must be enabled because until it is licensed the FortiGate VM supports only low-strength encryption. HTTPS access will not work.

For example:

```

config system interface
edit port1
set ip 192.168.0.100 255.255.255.0
append allowaccess http
end

```



You can also use the `append allowaccess` CLI command to enable other access protocols, such as `auto-ipsec`, `http`, `probe-response`, `radius-acct`, `snmp`, and `telnet`. The `ping`, `https`, `ssh`, and `fgfm` protocols are enabled on the `port1` interface by default.

4. To configure the default gateway, enter the following CLI commands:

```

config router static
edit 1
set device port1
set gateway <class_ip>
end

```



You must configure the default gateway with an IPv4 address. FortiGate VM needs to access the Internet to contact the FortiGuard Distribution Network (FDN) to validate its license.

5. To configure your DNS servers, enter the following CLI commands:

```
config system dns
  set primary <Primary DNS server>
  set secondary <Secondary DNS server>
end
```



The default DNS servers are 208.91.112.53 and 208.91.112.52.

6. To upload the FortiGate VM license from an FTP or TFTP server, use the following CLI command:

```
execute restore vmlicense {ftp | tftp} <VM license file name> <Server IP or FQDN>
[:server port]
```



You can also upload the license in the FortiGate VM Web-based Manager. See [Set FortiGate VM port1 IP address on page 61](#).

Web-based Manager and Evaluation License dialog box

The screenshot displays the FortiGate VM Web-based Manager interface. On the left is a navigation menu with categories like System, Network, Admin, and Router. The main area shows system information and resources. An 'Evaluation License' dialog box is open in the center, displaying the Fortinet logo and the following text:

FORTINET
REAL TIME NETWORK PROTECTION
FortiGate-VM
You are currently in evaluation mode
14 days until expiration

Below the dialog box, the 'License' section is visible, showing details for the VM License:

Registration Status	Valid [Update]
CPU's Detected	1 / 1
Evaluation License	Sat May 4 07:39:00 2013
Expires	

Below the license details, the 'Support Contract' and 'FortiGuard Services' sections are visible, both showing 'Unreachable' status with configuration links.

Connect to the FortiGate VM Web-based Manager

When you have configured the port1 IP address and netmask, launch a web browser and enter the IP address that you configured for port1. At the login page, enter the username `admin` and password field and select **Login**. The default password is no password. The Web-based Manager will appear with an **Evaluation License** dialog box.



Due to low encryption on the FortiGate side of the connection, some modern browsers will not allow the connection. If that is the case, the adjusting of the browser settings is unlikely to make a difference. There are two options:

- Use FTP or TFTP to apply the license
- Make sure that the interface on the port being accessed has been configured to allow HTTP/HTTPS access

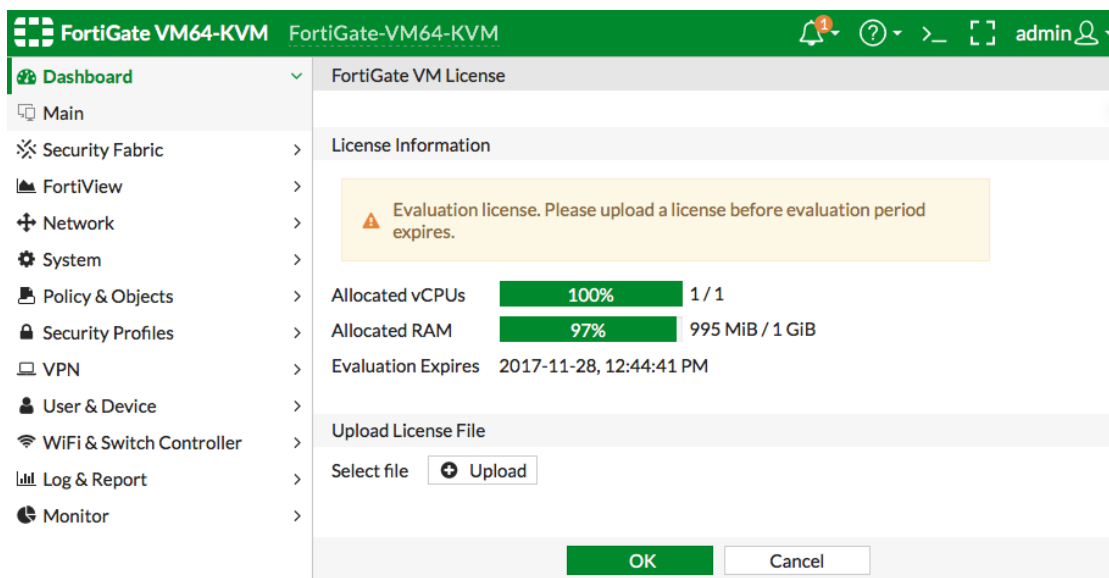
Upload the FortiGate VM license file

Every Fortinet VM includes a 15-day trial license. During this time the FortiGate VM operates in evaluation mode. Before using the FortiGate VM you must enter the license file that you downloaded from the [Customer Service & Support](#) website upon registration.

To upload the FortiGate VM licence file:

1. In the **Evaluation License** dialog box, select **Enter License**.
The license upload page opens.

License upload page:



2. Select **Upload** and locate the license file (.lic) on your computer. Select **OK** to upload the license file.
3. Refresh the browser to login.
4. Enter `admin` in the Name field and select **Login**. The VM registration status appears as valid in the License Information widget once the license has been validated by the FortiGuard Distribution Network (FDN) or FortiManager for closed networks.



Modern browsers can have an issue with allowing connecting to a FortiGate if the encryption on the device is too low. Adjusting browser settings does not normally mitigate the issue. If this happens, Admins must use a FTP/TFTP server to apply the license.

CLI

You can also upload the license file via the CLI using the following CLI command:

```
execute restore vmlicense [ftp | tftp] <filename string> <ftp server>[:ftp port]
```

Example:

The following is an example output when using a tftp server to install license.

```
exec restore vmlicense tftp license.lic 10.0.1.2
This operation will overwrite the current VM license!Do you want to continue? (y/n)y
Please wait...Connect to tftp server 10.0.1.2 ...
Get VM license from tftp server OK.
VM license install succeeded.
Rebooting firewall.
```



The command has the side effect of rebooting the firewall without giving you a chance to back out or delay the reboot, so be careful about the timing of using the command.

Validate the FortiGate VM license with FortiManager

You can validate your FortiGate VM license with some models of FortiManager. To determine whether your FortiManager unit has the VM Activation feature, see Features section of the [FortiManager Product Data sheet](#).

To validate your FortiGate VM with your FortiManager:

1. To configure your FortiManager as a closed network, enter the following CLI command on your FortiManager:

```
config fmupdate publicnetwork
  set status disable
end
```
2. To configure FortiGate VM to use FortiManager as its override server, enter the following CLI commands on your FortiGate VM:

```
config system central-management
  set mode normal
  set type fortimanager
```

```

set include-default-servers disable
set vdom <Enter the name of the VDOM to use when communicating with the FortiManager
device>
config server-list
edit 1
set server-type update rating
set server-address <your FMG IP>
next
end
end

```

3. Load the FortiGate VM license file in the Web-based Manager.

- Go to **System > Dashboard > Status**.
- In the **License Information** widget, in the **Registration Status** field, select **Update**. Browse for the `.lic` license file and select **OK**.

4. To activate the FortiGate VM license, enter the following CLI command on your FortiGate VM:

```
execute update-now
```

5. To check the FortiGate VM license status, enter the following CLI commands on your FortiGate VM:

```
get system status
```

The following output is displayed:

```

Version: Fortigate-VM v5.0,build0099,120910 (Interim)
Virus-DB: 15.00361(2011-08-24 17:17)
Extended DB: 15.00000(2011-08-24 17:09)
Extreme DB: 14.00000(2011-08-24 17:10)
IPS-DB: 3.00224(2011-10-28 16:39)
FortiClient application signature package: 1.456(2012-01-17 18:27)
Serial-Number: FGVM02Q105060000
License Status: Valid
BIOS version: 04000002
Log hard disk: Available
Hostname: Fortigate-VM
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Distribution: International
Branch point: 511
Release Version Information: MR3 Patch 4
System time: Wed Jan 18 11:24:34 2012

```

```
diagnose hardware sysinfo vm full
```

The following output is displayed:

```

UUID: 564db33a29519f6b1025bf8539a41e92
valid: 1
status: 1
code: 200 (If the license is a duplicate, code 401 will be displayed)
warn: 0
copy: 0
received: 45438
warning: 0

```




Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.